AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 112–152

PRIVACY AND DATA SECURITY: PROTECTING CONSUMERS IN THE MODERN WORLD

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

JUNE 29, 2011

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

71–313 PDF WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

JOHN D. ROCKEFELLER IV, West Virginia, *Chairman*

DANIEL K. INOUYE, Hawaii	KAY BAILEY HUTCHISON, Texas, *Ranking*
JOHN F. KERRY, Massachusetts	OLYMPIA J. SNOWE, Maine
BARBARA BOXER, California	JIM DEMINT, South Carolina
BILL NELSON, Florida	JOHN THUNE, South Dakota
MARIA CANTWELL, Washington	ROGER F. WICKER, Mississippi
FRANK R. LAUTENBERG, New Jersey	JOHNNY ISAKSON, Georgia
MARK PRYOR, Arkansas	ROY BLUNT, Missouri
CLAIRE MCCASKILL, Missouri	JOHN BOOZMAN, Arkansas
AMY KLOBUCHAR, Minnesota	PATRICK J. TOOMEY, Pennsylvania
TOM UDALL, New Mexico	MARCO RUBIO, Florida
MARK WARNER, Virginia	KELLY AYOTTE, New Hampshire
MARK BEGICH, Alaska	DEAN HELLER, Nevada

ELLEN L. DONESKI, *Staff Director*
JAMES REID, *Deputy Staff Director*
BRUCE H. ANDREWS, *General Counsel*
BRIAN M. HENDRICKS, *Republican Staff Director and General Counsel*
TODD BERTOSON, *Republican Deputy Staff Director*
REBECCA SEIDEL, *Republic Chief Counsel*

CONTENTS

	Page
Hearing held on June 29, 2011	1
Statement of Senator Rockefeller	1
Statement of Senator Kerry	2
Statement of Senator Toomey	4
Prepared statement of the National Retail Federation and Shop.org	6
Statement of Senator Wicker	36
Statement of Senator Ayotte	36
Statement of Senator Klobuchar	38

WITNESSES

Hon. Julie Brill, Commissioner, Federal Trade Commission	13
Prepared statement	15
Hon. Cameron F. Kerry, General Counsel, U.S. Department of Commerce	23
Prepared statement	24
Austin C. Schlick, General Counsel, Federal Communications Commission	29
Prepared statement	31
Stuart K. Pratt, President and CEO, Consumer Data Industry Association	40
Prepared statement	42
Ioana Rusu, Regulatory Counsel, Consumers Union	46
Prepared statement	48
Tim Schaaff, President, Sony Network Entertainment International	52
Prepared statement	53
Thomas M. Lenard, Ph.D., President and Senior Fellow, Technology Policy Institute	55
Prepared statement	56
Scott Taylor, Chief Privacy Officer, Hewlett-Packard Company	59
Prepared statement	60

APPENDIX

Letter, dated June 29, 2011, to Hon. John D. Rockefeller IV and Hon. Kay Bailey Hutchison from: American Advertising Federation, American Association of Advertising Agencies, Association for Competitive Technology, Consumer Data Industry Association, CTIA—The Wireless Association, Direct Marketing Association, Electronic Retailing Association, Interactive Advertising Bureau, National Association of Professional Background Screeners, National Business Coalition on E-Commerce and Privacy, NetChoice, Network Advertising Initiative, Performance Marketing Association and U.S. Chamber of Commerce	69
Letter, dated June 27, 2011, to Natasha Mbabazi, Senator Thomas Udall, Senator Frank Lautenberg and Senator Barbara Boxer from Lisa Liberi and Lisa Ostella	72
Response to written questions submitted to Hon. Julie Brill by:	
Hon. John D. Rockefeller IV	73
Hon. Claire McCaskill	74
Hon. John F. Kerry	74
Hon. Barbara Boxer	77
Hon. Mark Begich	78
Hon. Kelly Ayotte	79
Response to written questions submitted to Hon. Cameron F. Kerry by:	
Hon. John F. Kerry	81
Hon. Mark Begich	83

Page

Response to written question submitted to Austin C. Schlick by:
Hon. Claire McCaskill 84
Hon. Mark Begich 84
Response to written questions submitted to Stuart K. Pratt by:
Hon. John D. Rockefeller IV 85
Hon. Roger F. Wicker 87
Response to written question submitted to Ioana Rusu by:
Hon. John D. Rockefeller IV 87
Hon. Barbara Boxer 89
Response to written questions submitted to Tim Schaaff by:
Hon. Claire McCaskill 90
Response to written questions submitted to Thomas M. Lenard, Ph.D. by:
Hon. Roger F. Wicker 91

PRIVACY AND DATA SECURITY: PROTECTING CONSUMERS IN THE MODERN WORLD

WEDNESDAY, JUNE 29, 2011

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10 a.m. in room SR–253, Russell Senate Office Building, Hon. John D. Rockefeller IV, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. JOHN D. ROCKEFELLER IV, U.S. SENATOR FROM WEST VIRGINIA

The CHAIRMAN. We've got to begin. This hearing will come to order. This is the third hearing on consumer privacy that we've had in this committee in the 112th Congress. As I have repeatedly emphasized, Americans are often unaware of the vast amounts of information that are being collected on them and then used usually to their detriment.

I've focused on the need for companies to provide everyday consumers with a clear understanding of what information they are collecting, where the information is going, and how it's being used. I've also asked companies to give consumers an easy way for them to stop those collection processes. I don't think this is too much to ask of companies that are making a lot of money and a lot of money that comes off of consumers' personal information.

That should not be happening in America. This is a new cost of doing business in America, and people have to understand that. Government doesn't subsidize what companies need to be doing to protect privacy.

Poll after poll shows that Americans are increasingly concerned about their loss of privacy, and these same polls show that Americans don't know what to do about it. I've had endless meetings in my state, as I'm sure Senator Kerry and Senator Toomey have, also. They don't know what to do about it.

It's my intent, as Chairman of this Committee of jurisdiction—and I say that very clearly for many to hear—to change all of this. I want ordinary consumers to know what is being done with their personal information, and I want to give them the power to do something about that.

That is why I've introduced S. 917, the Do-Not-Track Online Act of 2011. This bill is based on a very simple concept. With an easy click of the mouse, consumers can tell all online companies they do not want their information collected, period. One click, no informa-

tion collected. Under my bill, companies would be obliged to honor that request. It's that simple.

Senator Kerry has also introduced a bill, S. 799, the Commercial Bill of Rights Act of 2011, which is a very comprehensive piece of legislation that governs many facets of all of this and of the economy, indeed. It's a very good piece of legislation.

And other members of the Committee have similarly voiced strong interest in privacy matters. I believe these hearings form the basis for building bipartisan consensus about really doing something about this.

Now, today's hearing is also about data security, which directly implicates consumer privacy. We are reminded of this, I'm afraid, every day in the headlines.

The recent security breaches at Citibank, Sony, and Epsilon show that companies are increasingly vulnerable to cyber attacks that compromise the safety and the privacy of Americans. I'm not concerned about the breaches. I'm concerned about what happens to American people as a result of that. Well, I'm concerned about the breaches, too.

When criminals break into a database and steal credit card numbers, Social Security numbers, or even e-mail addresses, they can use this information to commit identity theft, which can have devastating consequences for the victims.

That is why Senator Pryor and I have introduced once again this year, S. 1207, the Data Security and Breach Notification Act, the same bill that we introduced in the last Congress. The bill will impose an obligation on companies to adopt basic security protocols to protect sensitive consumer data, and it would further require these companies to notify affected consumers in the wake of a security breach—again, a cost of doing business in the New World.

The bill would also require greater transparency for something called the data broker industry, not one of my favorite subjects to talk or think about. These are companies that amass vast amounts of data on consumers, sell that information to other companies, usually for marketing purposes, and they make a lot of money for it. Most people don't even know they exist. They've never heard of them. They have no idea that their privacy is being invaded, used, sold, and marketed.

So there's a broad consensus that federal data security legislation is necessary. The Administration included a breach notification provision similar to the provision of S. 1207, Pryor's and my bill, in its cyber security proposal. In order for this bill to be ready for floor consideration as part of the larger cyber security effort, I will work with Senator Pryor and all of my colleagues to make sure that all of this works out.

I now call on Senator Kerry. I warn you we have some votes at 11, so we're going to be hurrying just a bit.

STATEMENT OF HON. JOHN F. KERRY,
U.S. SENATOR FROM MASSACHUSETTS

Senator KERRY. Indeed, and, Mr. Chairman, in that spirit, I'll try to be very quick, because we do have about five votes, I think, coming up.

First of all, thank you for holding this hearing. And I want to thank you for the meeting that we had the other day to discuss, not just our bill, but the whole approach of the Committee. And I pledge to work with you as closely as possible as we try to find a broad-based and, hopefully, consensus approach to the challenges of this issue.

What we're discussing today is really the ability of people to sort of control or have some impact on the way profiles about them—a digital profile or multiple digital profiles—are compiled on almost all of us and then sliced and diced and traded in a marketplace where many people are not, as you have just remarked, appropriately in control of what happens to them.

We also are here to discuss the need to establish uniform standards for the security of the private networks that hold our information. Now, when I talk about privacy, I'm talking about the ability of people to exercise choice and control over how their information—I repeat, their information—is collected, used, and distributed.

Data security is a subset of that issue and about how companies can secure the information that they collect on people and what they need to do in the case of a security lapse. Both are serious matters.

When a company is hacked, and the information of hundreds of thousands of their consumers is taken, the individuals whose information is revealed are obviously exposed to the risk of the hackers who stole it using that information in any number of ways, but particularly to harm them. The company that is hacked is hurt by being exposed to reputational damage and harmed relations with its customers.

And establishing uniform procedures for how to react in the case of a security lapse and increasing incentives for having strong security procedures is, I think, a necessary goal and well addressed in the data breach legislation that you, Mr. Chairman, and Senator Pryor have introduced.

But data security requirements alone are not going to give people authority over how their information is collected or its use and distribution. Data security is just one piece of the overall privacy puzzle.

After working with Senator McCain and others for some months on this issue—you mentioned the legislation, Mr. Chairman, a moment ago that we've introduced, and I appreciate your comments about it. We need to find a way to meld the various approaches that are out there and to build, obviously, a consensus within this committee—I agree with you, the Committee of jurisdiction—in order to be able to protect people.

Beyond accountability security, I think that the legislation we've contemplated is going to give people meaningful and specific explanations and control on how their information is being collected, used, and distributed, as well as, importantly, the power to opt-out of those practices.

I think Senator Rockefeller's approach is a good one, a strong one, an important one, the Do-Not-Track. It's one component of it. But I do think that beyond that, we still have to deal with this

question of choice over how your information is managed even if you do consent to it.

And so I think that what we've put forward is a comprehensive bipartisan proposal as a starting point.

And, Mr. Chairman, I think it's critical to work with you, Senator Kay Bailey Hutchison, Senator Snowe, and others on the Committee, in order to bring more people to the table, and I certainly look forward to doing that.

I do want to point out that at the moment, sort of in the center of this debate—there are a couple of polls, but in the center, you've got major companies, like Intel, Microsoft, eBay, Hewlett-Packard, as well as consumer advocates represented by the Consumers Union and others who are helping us to try to focus this in the right direction.

And, finally, you know, we have expert agencies represented here today. The Federal Trade Commission, the Department of Commerce, the Federal Communications Commission—they've all been doing what they can to protect Americans using the legal tools available to them and using their ability to convene the stakeholders and the experts and then educate themselves and consumers on the changing practices in this rapidly moving and ever evolving world we live in.

But the fact is that they don't have all the tools necessary. And that's why this discussion is so important.

So I look forward to working with you, Mr. Chairman, making sure we have a complete picture of what is going on in the market today from which we can draw the best conclusions about how to proceed to have a smart, baseline, commercial privacy protection put into law. And I thank you for focusing intently on this important issue.

The CHAIRMAN. Thank you, Senator Kerry.

Senator Toomey.

STATEMENT OF HON. PATRICK TOOMEY,
U.S. SENATOR FROM PENNSYLVANIA

Senator TOOMEY. Thank you very much, Mr. Chairman, for holding another hearing on this very important topic. I appreciate that, and I agree with Senator Kerry's characterization that data security is one subset of consumer privacy, which is itself, though, a very broad topic.

On data security, there seems to be broad support among industry stakeholders, consumer advocates, and many Members of Congress for a national standard. And it's certainly an issue that Congress is likely to address legislatively in the near future.

In recent years, there have been a number of high profile data breaches affecting consumers nationwide. And establishing a single federal standard for notifying victims of data breaches and protecting sensitive information is something I do think we should consider seriously.

I look forward to working with the Chairman and other members of the Committee in, hopefully, addressing this in a constructive and bipartisan manner.

On the broader issue of privacy, however, I'm not sure there is yet a consensus on how to best protect consumers or whether a leg-

islative solution is, indeed, the best method for doing so. So before Congress considers comprehensive privacy legislation that would have a significant impact on businesses large and small and on consumers, I think we need to thoroughly examine this issue and make sure that we don't apply a solution in search of a problem.

I'm very interested to hear from our witnesses today on what, specifically, is most concerning to consumers when it comes to privacy; what consumers' expectations are regarding their privacy; and what, if any, real harm has occurred from online data collection and how to best address any such harms. In a world where millions of people voluntarily share very personal information on websites like Facebook and Twitter on a daily basis, I'm not sure exactly what consumer expectations are when it comes to privacy. But I am pretty sure that different consumers have different expectations about privacy.

I'm also not sure who's best suited or even qualified to make the determination. Should it be Congress? Should it be the Federal Trade Commission? Or neither? Perhaps industry and consumers should set the standard by mutual consent in their interactions.

These are the issues that I hope we will carefully examine. And I'm hopeful that we can make some progress on them today.

My colleagues who have introduced legislation in this field are certainly very well-intentioned and its thoughtful legislation. But I am not sure that we've fully considered the unintended consequences that could attach to these proposals.

The Internet and the communications marketplace have flourished and fueled tremendous economic growth in part because excessive government regulation has not yet occurred. In fact, American innovation in this field far outstrips the innovation that's occurring in other places, including Europe, where much more extensive regulation currently exists.

So, the Internet clearly has changed the way we communicate and do business very much for the better. And we should be careful about imposing new rules and regulations that might unnecessarily harm future innovations.

I'm sure no one on this committee wants to "break the Internet" or limit many of the popular online services consumers can access. In order to avoid fundamentally altering the current online experience, and creating these unintended consequences, I just urge that we all proceed with caution.

One very brief example, for instance—overly restrictive regulations for online advertising would likely result in consumers having access to fewer free online services and applications. I'm not sure that we're qualified at this point to make the judgment of what that trade-off ought to be.

I want to protect privacy online, and I want consumers to feel comfortable when using the Internet. But until we have a clear picture of the harm we're trying to address and have looked at a cost-benefit analysis of any new privacy legislation, I have reservations about moving forward with a legislative mandate.

That said, there are a number of ideas that have been put on the table that I do find appealing. One example is the idea that maybe we ought to consider consolidating privacy enforcement and oversight into a single federal agency rather than multiple agencies.

So on this and this entire range of topics, I look forward to working with you, Mr. Chairman, and the other members of the Committee. Again, I thank you for holding this hearing. And I'd like to ask consent to have a statement prepared by the National Retail Federation included in the record.

[The information referred to follows:]

PREPARED STATEMENT OF THE NATIONAL RETAIL FEDERATION AND SHOP.ORG

Chairman Rockefeller, Ranking Member Hutchison and members of the Senate Committee on Commerce, Science, and Transportation, on behalf of the National Retail Federation and its division Shop.org, I appreciate the opportunity to submit this written statement to the Committee in connection with its hearing entitled "Privacy and Data Security: Protecting Consumers in the Modern World" held on June 29, 2011.

As the world's largest retail trade association, the National Retail Federation's global membership includes retailers of all sizes, formats and channels of distribution, as well as chain restaurants and industry partners from the U.S. and more than 45 countries abroad. In the United States, NRF represents the breadth and diversity of an industry with more than 1.6 million American companies that employ nearly 25 million workers and generated 2010 sales of $2.4 trillion. Shop.org, a division of the National Retail Federation, is the world's leading membership community for digital retail. Founded in 1996, Shop.org's 600 members include the 10 largest online retailers in the U.S. and more than 60 percent of the *Internet Retailer* Top 100 E-Retailers.

I. Introduction: Information is the Lifeblood of Retail Success and Growth

Retailers are by their very nature marketers and advertisers. Consumer information used for these purposes is the lifeblood of the industry, and the catalyst for its growth. Trends and revolutions in retailing, such as the rise of e-commerce, are fueled by the sharing of information between merchants and their customers. The information collected by retailers ensures the right merchandise is stocked on shelves, customers are offered the best sales and promotions to get them in the door, and stores are opened in locations where demand is the highest, to name just a few of the important uses of consumer information.

As businesses that have direct, first-party relationships with their customers, retailers understand why the gathering and use of some customer information for these and other lawful purposes may still raise consumer privacy concerns despite the clear benefits that the smart use of information has provided to consumers over the years. Indeed, privacy and security considerations are of paramount concern to retailers for that very reason, and their goals are to be as responsive to consumer concerns as possible. In a very competitive industry that averages only 2 percent profit margins, retailers distinguish themselves on the quality of their customer service and the shopping experience they provide. Protecting customers' information is an important part of that mission.

Furthermore, we agree with the Committee that privacy considerations should be taken seriously by all businesses—from securing important human resources information to protecting databases that hold sensitive customer information. However, we also believe that some of the legislative proposals being considered by the Committee go too far in restricting customary and lawful uses of information that are essential to retail businesses, and we are concerned that some of the provisions could have the unintended effect of stifling innovation and growth in our industry at a critical time for our economy and the retail sector as a whole.

II. The Continuing Growth of E-Commerce as a Retail Channel

Retailers have spent the last fifteen years revolutionizing the way Americans shop by giving each and every consumer greater access to a wide variety of brands, goods, and services at highly competitive prices both in their stores and online. E-commerce has brought millions of new customers to retailers' virtual stores and has also served to increase new customer traffic in traditional brick-and-mortar shops as well. According to the Shop.org-released annual study, The State of Retailing Online ("SORO"), conducted each year by Forrester Research, Inc., online retail sales soared to $156 billion in 2009 and are projected to likely exceed the $200 billion mark in 2012.[1]

[1] The State of Retailing Online 2009.

As retailers continue to fine-tune their selling and marketing strategies, consumers, in particular, have become more comfortable shopping online—especially with retailers that they know and trust. By the end of 2009, online sales accounted for 6 percent of all retail sales.[2] In contrast, it took the catalog industry *100 years* to represent just 4.7 percent of all retail sales.[3] What has made this online retail revolution possible is the widespread access to the Internet and e-mail by American consumers, *and* the ability for retailers to actively and nimbly adapt to their customers' evolving shopping preferences. Retailers are constantly re-designing and adding new features to their online sites, striving to create the most relevant content and consumer-friendly web experiences for their customers. This helps retailers maintain their customer base, draw in new shoppers, and improve overall conversion rates. As noted previously, retailers *must be relentless* about delivering the most compelling and relevant experience to their customers because that is how they differentiate themselves in an extremely competitive, volume-driven business that operates on low profit margins.

The key to the constant evolution of retail marketing and sales is the information that retailers have collected about their customers' shopping preferences in stores and on their websites over time. That being said, retailers take their customers' privacy and security seriously and have an excellent track record of using customer information in order to deliver *relevant and targeted* marketing. Retailers have long understood that keeping their customers happy is the most essential part of building positive long-term business relationships. However, retailers do not want to fundamentally alter an entire medium for effective information collection and use. We believe that effective and enforceable self-regulation and, in the case of retailing, industry leadership (or "best practices"), are among the most effective ways to protect consumers while still enabling businesses to maintain the flexibility to innovate and adopt new technologies to better serve their customers.

There is an old saying that "the customer is always right," and that could not be truer in the retail industry as retailers must meet customers' constantly evolving expectations. If they do not meet their customers' expectations or, worse, violate their trust, customers will not be happy and they will shop elsewhere. Given the limitless number of shopping choices presented to American consumers every day, particularly online, there's a new saying in online retail that is particularly appropriate in this context: "Competition is only one click away."

With retailers' interests aligned with their customers' interests in terms of satisfying their needs and allaying their concerns, honoring consumers' privacy and marketing preferences and securing their data is of paramount importance. For this reason, retail customers are very likely to have their privacy and security expectations met and they continue to maintain significant control over the business relationship. The Federal Trade Commission ("FTC") recognized as much in its December 2010 staff report on a proposed U.S. privacy framework (the "FTC Privacy Report"), noting that it had less concerns about these types of consumer information practices than others.[4]

III. Views on Proposed Data Security Provisions in Current Legislation

There are many ways that retailers are currently securing information as well as protecting sensitive customer information. First, to the extent that retailers act as credit grantors, they must abide by the statutory privacy and data security protections required by the Gramm Leach Bliley Act ("GLBA"), The Fair Credit Reporting Act ("FCRA"), and the Fair and Accurate Credit Transactions Act ("FACTA"). Further, any retailer that processes and retains third-party credit card information is currently subject to the Payment Cards Industry ("PCI") standards program developed by Visa, MasterCard, American Express and Discover. These statutes and programs do not apply to non-sensitive marketing data, as their goal is to provide important protections for consumers' most sensitive financial data because its misuse may lead to identity theft or other significant financial harm.

A. Data Minimization and Retention

While we generally support legislation that would create uniform national data security standards, some of the proposed provisions in privacy and data security bills, such as data retention standards, would be problematic. We also agree that non-sensitive customer data should be protected as part of proposed data security standards, but believe that such protection must be proportionate to the type and

---

[2] *Id.*

[3] The State of Retailing Online 2002.

[4] *See* Preliminary FTC Staff Report, "Protecting Consumer Privacy in an Era of Rapid Change," December 1, 2010 (hereinafter, "FTC Privacy Report").

sensitivity of the data. A few examples here may be helpful for the Committee's review and consideration.

First, provisions that would require deletion of data unless there is a legitimate business need for continued retention must be flexible, as the needs will vary greatly from business to business, and companies should not be subject to arbitrary time limits for how long data can be stored. Retailers, for instance, have many legitimate uses for customer data, from fraud prevention to inventory planning, to planning marketing campaigns and store openings. As a result, we believe data retention determinations must be left to the business itself. In fact, in the 46 states and 3 federal territorial jurisdictions that have recently enacted data security and breach notification statutes, none have legislated a specific time period for data retention and we would urge Congress to do as these states and jurisdictions have done.

Additionally, while the FTC Privacy Report advises that data retention periods should be linked in some way to the type or sensitivity of the data being collected, this should not force retailers to arbitrarily dump marketing information that they have expended significant resources to develop and that may be relevant to their businesses in the future. For example, innovations in retailing and e-commerce are fueled by data analytics and other widely used Customer Relationship Management ("CRM") techniques that rely heavily on complete and reliable sources of information. Congress should therefore be cautious in setting one-size-fits-all retention periods for industry that could have the significant unintended consequence of forcing the removal of critical data from businesses that, in turn, may limit their future market growth and ability to compete when innovative new uses for that information are later developed.

In addition to marketing, data retention is necessary to provide customers with a seamless experience. For instance, if a customer purchases a couch from a retailer and then 24 months later would like to complete the set, it is critical for the retailer to have all of the information about the initial purchase stored in its system in order to provide the customer with the service that customer expects and to which they have become accustomed. The time period for a retailer wishing to provide good customer service is dependent upon the retailer's reasonable expectations and experience concerning its typical customers' needs.

B. Accuracy, Access and Correction Rights for Non-Sensitive Data

We disagree with proponents of data security legislation who believe businesses should be required to ensure the absolute accuracy of non-sensitive marketing data that they collect under the mistaken premise that it might result in a customer not receiving an important benefit. Information that is used to determine eligibility for credit, employment, housing, insurance, and other important financial services, is certainly the type of information that may cause economic harm if its inaccuracy leads to a denial of such service. However, information accuracy, access and correction rights are already provided for this type of sensitive information under several federal laws, including FCRA and FACTA.

With respect to non-sensitive marketing data, it is certainly in a retailers' best interest to have generalized information about their customers' product interests in order to send them the most relevant marketing, but marketing files do not merit the same level of scrutiny as credit and financial information because, by their very nature, this non-sensitive information is not used to deny consumers important benefits (such as credit, employment, housing, or insurance). Moreover, even moderate inaccuracy of non-sensitive marketing information (*e.g.,* an incorrect sock size or color preference) typically cannot cause significant economic harm to an individual in the same way that the denial of credit, employment, housing and insurance might.

For these reasons, we would advise that the Committee reconsider the inclusion of accuracy, access and correction rights for non-sensitive marketing information in any proposed data security or privacy legislation. On the other hand, as a matter of good practices, we do believe that access to customer information should generally be restricted to those with an articulable business "need to know."

C. Private Rights of Action

We appreciate that none of the proposed data security or privacy bills being considered by the Committee establish new private rights of action as part of their enforcement regime. As the Committee can appreciate, retailers are already subject to massive fines and expenses for data security violations under actions by the Federal Trade Commission, state attorneys general and private entities (for PCI standards enforcement)—costs which collectively run into the millions of dollars. In its consideration of the Committee's legislation, we strongly urge Congress not to amplify

these costs by also subjecting every American business that accepts a credit card to the potential ruinous compounding of additional private litigation.

IV. Views on Proposed Privacy Provisions in Current Legislation

A. Scope of Covered Information

The scope of legislative proposals to protect consumer privacy has often been a key issue for retailers and is again a factor that we urge the Committee to carefully consider. In proposed legislation, the definitions of covered information (where provided and not left to the discretion of the FTC) are often overly inclusive of non-sensitive and even non-personal information. For example, as currently drafted, the Kerry-McCain privacy bill would cover nearly all data collected for commercial use, no matter how sensitive or innocuous, if that data can be linked to a specific consumer, computer or device.

Additionally, while the legislative language states that it covers all commercial entities that collect data in both online and offline contexts, the statements of Senator Kerry and the testimony offered at the Committee's privacy hearings this year have focused more keenly on online data collection and the provision of consumer choice in these channels. Given that the offline collection of consumer data is much more layered than online collection, and that offering consumer notices and choice mechanisms offline will be much more onerous on businesses and consumers alike, we strongly suggest that legislative proposals be narrowed to simply address significant known consumer protection concerns and not be crafted as one-size-fits-all proposals intended to cover every possible instance in which data—particularly non-personally identifiable data—is collected in the course of doing business. To do so would be tantamount to regulating *all* information in our information economy, which we believe would have significant unintended consequences.

Moreover, the proposed broadening of the definition of "covered information" in the bill to include data that is not personally identifiable information ("PII") is troubling. The FTC Privacy Report concluded that "any data that relates to a person has privacy implications and, therefore, should be protected appropriately."[5] However, having a proposed privacy framework whose scope would be broadly defined to cover any data that can be "linked" to a consumer, computer or mobile device is one that is as broad as covering *all* data itself, since any data can be conceivably linked to any other data in a database. The implied breadth of regulation in the FTC Privacy Report goes well beyond the agency's consumer protection mandate and, in terms of practicality, is simply untenable.

The Commission also noted that the ability to re-identify customers from anonymous data has caused the traditional understanding of PII to lose significance. However, in the examples the FTC presents in the report, the companies involved were either violating their own privacy policies or the policies of the company that hired them. These types of corporate transgressions should be properly handled under the FTC's currently authorized enforcement regime, and not become the stated cause for the complete redefinition of what has traditionally been considered PII. Furthermore, maintaining a carefully crafted definition of covered information based on the same concepts of PII that underlie current federal privacy laws would provide some natural boundary to proposed privacy legislation so that the scope of new government regulations for consumer protection purposes is tied to data that actually identifies consumers.

B. Exceptions for Common First-Party and Third-Party Practices

The first-party marketing exception is extremely important to retailers in all marketing channels.[6] Retailers have been advertising and marketing to their own customers since retail began. A century ago, pioneering general stores kept careful logs of what customers bought, and often extended simplified credit "terms" or deferred payment based on the shopping histories of loyal customers. In towns and cities, local haberdashers knew their customers' measurements and preferences by heart, and neighborhood pharmacies were places where simple medical advice was dispensed while the community gathered at the lunch counter to share news and connect. What was once face-to-face interaction with a brick-and-mortar small business has, over time, evolved in to customer loyalty programs such as those found at a favorite grocer, department store, and on popular websites known for serving up targeted customer recommendations and providing one-click ordering services.

---

[5] FTC Privacy Report, p. 39.

[6] Whether legislation narrows the scope of the exception to only cover the online collection of data is significant, as first-party marketing is a vital tool to retailers in multiple channels including, in-store, catalog, online and mobile.

In the FTC Privacy Report, the Commission asked if first-party marketing should be limited to the context in which the data is collected from the consumer, and the Kerry-McCain bill limits the exception in certain similar ways. Our view is that the online or offline channel in which first-party marketing is conducted should *not* cause the exception to be narrowed to the use of information collected only in that channel because a customer's common understanding is that he or she is doing business with a single retailer, even if that interaction happens in one of several available mediums. A few examples here again may be helpful to the Committee.

As the Committee knows, retailers operate across all channels and consumers have come to expect a seamless shopping experience whether they are browsing the retailer's site online or on their mobile device, or browsing the store's aisles at the local shopping center. Consumers do not differentiate or segment out their experiences with a retailer, and retailers must accommodate their expectations. Integrating online and offline consumer information allows retail customers to enjoy integrated services, such as in-store returns for online purchases, and the ability to shop with loyalty points and coupons through the medium that is most convenient for them. It also allows for the deployment of new technologies such as in-store kiosks that permit online ordering or allow customers to manage their wedding and baby registries or personalized "wish lists." Customers often appreciate receiving marketing promotions in several different ways as well. For those customers whose preferences are specific, opt-outs for mail and e-mail can be easily obtained under current law and marketing self-regulation programs. It is also well-known that reputable retailers respect customer preferences as a matter of good customer service.

Again, whether a customer shops in-store, online, through a mobile application or by catalog, that consumer's assumption is that they are shopping with a single retailer. The first-party marketing exemption should be extended to cover all of these environments in which retailers interact with their own customers. Additionally, the exception should cover customer marketing information that is shared with affiliates as well as third-parties who are operating seamlessly within the four walls of the retail operation, such as leased departments or in-home services.

For example, some retailers have launched integrated websites where customers can switch from one brand to the next easily. A few are even utilizing common shopping carts and web-based check-out services, truly tying together their business lines. If an affiliate or service-provider exception were not included within the first-party marketing exception, it could seriously harm these growing programs. Additionally, department stores have historically relied on leased departments and other third-parties to provide their in-store customers with specialized, branded products (*e.g.,* cosmetics, sunglasses, jewelry, etc.) and additional customer services (*e.g.,* hair salons, photo studios, appliance repair, etc.). If these types of relationships are not considered within the scope of the first-party marketing exception, it could critically damage these relationships and force a complete reorganization of traditional retail department store practices that underlie the provision of these services—even possibly limiting their future availability to consumers.

The final question posed by the FTC Privacy Report about first-party marketing asks how the proposed framework should handle the process of data enhancement, whereby a company obtains information about its customers from other sources to enrich its customer databases. This practice should not be considered different from first-party marketing and thereby subject to enhanced notice-and-choice regulations, but should fall under similar exceptions for "first-party marketing." Data enhancement tools are used for many different purposes: customer relationship management (CRM), marketing (especially targeted marketing), internal business planning (*e.g.,* locating stores and planning inventory), loss prevention, fraud prevention and product and service fulfillment. For instance, if a retailer did not use third-party data enhancement to keep current with its customers, it could mistakenly send promotional coupons to a deceased customer's household without ever knowing it. By confirming current addresses with third-party service providers, a retailer also might avoid sending mail to an old address for products which may be unwanted or irrelevant to the new resident. Many consumers often do not bother updating their mailing address even with their favorite retailer, simply assuming they will continue to receive discounts and promotions from the same store at their new mailing address. In another example, retailers commonly run shipping addresses provided by a consumer against fraud prevention lists, and if new addresses raise red flags in the future, they may be subject to further scrutiny via data enhancement tools.

If these types of common data practices were to fall outside of the exceptions for commonly accepted practices in federal legislation, and be subject to a new customer notice-andchoice regime, what are now routine first-party processes would have to be noticed by retailers and customers would be constantly bombarded with mar-

keting "choices" at the point of sale, whether in a store, on the Internet, or on their mobile devices. This would be extremely disruptive to the retail customer experience and, furthermore, provides no conceivable benefit to consumers because these common practices are not ones that consumers are complaining about in the first place.

C. Offering Consumer Choice in the Context in Which It Is Made (Online and Offline)

The FTC Privacy Report states that to "be most effective, companies should provide the choice mechanism at a time and in a context in which the consumer is making a decision about his or her data."[7] Indeed, some suggest that allowing consumer choice is very technologically workable in the online context. It is true that technology has made real-time notice and choice regimes more palatable and, when taken individually, disruptions in the flow of the customer's experience may not seem like a big deal to a lay person. However, in terms of overall conversion rates, these types of "hiccups" or consumer annoyances can be devastating to retailers.

We all know how frustrating pop-ups can be when you are simply trying to read the latest headlines on a newspaper website. Now transfer that experience to a retail website, where customers have come to expect a seamless experience from homepage to check-out. Even under the best circumstances, average conversion rates are only about 3.1 percent and shopping cart abandonment rates still hover at 50 percent.[8] Any additional hurdles would simply serve to frustrate consumers and could drive down the number of completed transactions overall. Further, we now know from years of experience, even when offered the option, as required by law, consumers do not regularly take advantage of these types of programs. In fact, by our estimates, only 6 percent of retail customers exercised their right to opt-out of marketing e-mails in 2007.[9]

To further complicate matters, the FTC Privacy Report suggested, and the proposed federal legislation would require, notice and consent for the collection of information in-store if that information collection and use fell outside of the exceptions for commonly authorized uses. These types of point-of-sale notice requirements are extraordinarily burdensome on both the retailer and the consumer in a physical store environment. Would a store clerk at point of sale be required to make sure a customer both received a privacy policy and understood the choices offered to them? Would every clerk in a department store have to repeat the process as a consumer walked from one third-party administered leased department (*e.g.,* oriental rugs) to another (*e.g.,* cosmetics)? Additionally, what new and costly point-of-sale technology would be required to record a customer's marketing choices if they chose to opt-out? How would stores be required to keep track of that information ("durable opt-out") when customers can shop in hundreds of store locations in several, if not all, states, as well as online? Would a "John Smith" who exercised an opt-out in Oregon be recognized as the same John Smith who visited a store in Florida during a family vacation? Or what if John later logged onto the retail website or used a retail store's mobile application on his cell phone? With opt-out rates being historically low, would such investments even be worth the expense and employee training necessary, particularly given the number of temporary or seasonal employees retained by a retail store during the course of any given year?

With these considerations in mind, we ask that the members of the Committee reconsider this paradigm altogether and let these types of choices be exercised in the context in which a retail privacy policy is commonly offered. For instance, the Committee should consider allowing consumers to make marketing choices in the context of viewing a retailers' privacy policy on their website. In turn, we agree that marketers should make such policies more accessible to consumers—more easily found and in a simplified form.

The effect of inundating consumers with new notices is also compounded by the overly-broad definition of covered information contained in the Kerry-McCain legislation and the possibility that common practices such as data append or data enhancement are not exempt from these new notice requirements. To require customer choice for many activities that fall outside the bill's exceptions for commonly accepted practices—for example, transferring customer information for third-party data analytics, asking customers about the stage of their pregnancy (a medical condition) to market maternity clothes or baby gear, or even deploying cutting-edge mobile marketing technologies—will simply make these services much more difficult for retailers to continue to provide to their customers who want them.

---

[7] FTC Privacy Report, p. 58.
[8] The State of Retailing Online 2007, Part 1 of 2.
[9] The State of Retailing Online, 2008.

It is also important to mention again that consumers do not traditionally exercise choice—they rarely opt-in and they rarely opt-out. The proposed privacy legislation appears to force the issue, without perhaps fully considering the continual annoyance this may create for the average consumer. For many individuals, there is already annoyance about being forced to read and sign a health care privacy policy notice in a trusted doctor's office—and that policy covers the protection of their "sensitive" health information. Imagine the frustration if the web, or the checkout line in your favorite store, was littered with warnings about marketing information. Retailers can imagine, unfortunately, many customers exercising choices with their feet—by choosing to shop elsewhere rather than be frustrated by this government vision of a satisfying consumer shopping experience.

We are also concerned about federal legislative provisions that would require retailers to obtain opt-in consent for secondary uses of customer data that were not specifically disclosed at the time the data was first collected. We believe this requirement has the clear potential to stifle investment in future innovative uses of that data to benefit consumers. For example, had such a limitation been in place a decade ago, it may have prevented the use of data about customers' purchases to help provide recommendations to online shoppers (*e.g.,* suggestions that other customers viewing a particular product also viewed similar products, or a greater percentage of other customers favored one product over another). These recommendation services exist on many retail websites today and are strongly favored by online shoppers. The use of one customer's data to make online recommendations to other customers may not have been disclosed to consumers in the early stages of the development of these practices. Yet, online consumers have benefited from such innovations despite not having expressly *opted in* to these data uses in advance.

The appropriate choice standard for uses of marketing data and other non-identifiable or non-sensitive data is meaningful notice and the ability to opt-out, as many businesses currently provide. Otherwise, the well-meaning provisions in proposed legislation could result in actualizing the tragedy of the commons, whereby no innovation can take place to develop these beneficial services for customers because none of them have opted in to future data uses that permits their creation.

D. Do-Not-Track Mechanisms

We live in the "information age" as well as a consumer-driven economy where two-thirds of our nation's GDP is directly attributable to consumer spending. Stifling information flows and innovations in technology (such as mobile marketing) would have a very detrimental effect on newly rebounding retail sales. We are very concerned about the FTC's proposed "Do-Not-Track" mechanism, and question its relevancy in light of the recent launch of comprehensive self-regulatory programs (such as the Ad Choices program) or the new software being developed and incorporated into Internet browser software.

Despite its similar sounding name, a Do-Not-Track mechanism would be fundamentally different from each of its predecessor proposals—Do-Not-Call and Do-Not-Spam (which the FTC rejected)—in that the opt-out itself would not cover a specific phone number or individual's e-mail address, but instead could only be tied to computers or mobile devices that may be shared by multiple individuals within households or families. This shared use of devices would require individual consumers to continually opt-out as they changed devices (even moving from the many devices within their own home network: work computer, personal laptop, child's laptop, tower computer, Kindle, iPad, iPhone, Smartphone, and the list goes on) and could create significant consumer confusion because of the expectations built on the earlier Do-Not-Call program.

We urge the Committee to allow the new self-regulatory programs and technological solutions to take root and for the FTC to revisit this issue in its final privacy report only if such programs appear to be failing. Since self-regulatory programs exist already, we believe the FTC's efforts should be focused on consumer education and awareness (an area where the Commission has and *should* play a strong role), and not on whether consumers are actually exercising their right to opt out under such programs. As we have noted above, when offered choices, most consumers simply choose to take no action, even after information is made available to them. It is highly probable that, once again, the metrics from the new programs simply may not bear out the argument (or expectation) that consumers will opt-out even when given great information and tailored choices. We hope that both the Committee and the Commission will keep these considerations in mind as you and the FTC review the adequacy of existing self-regulatory programs and the necessity of mandating a government-run Do-Not-Track mechanism for consumers.

V. Conclusion

Retailers take the privacy and security of their customers' information seriously, and are motivated both by the desire to follow good business practices as well as a basic concern of maintaining their customers' satisfaction and not losing customers as the result of a perceived privacy gaffe or data security breach. We appreciate the Committee's focus on privacy and data security legislation and we believe that these continued hearings help clarify many of the issues surrounding the deployment of new and, sometimes controversial, technologies and business practices. As it has often been said, "sunlight is the best disinfectant," and an ongoing dialogue between the Committee and the business community over privacy issues is very useful. In particular, the Committee's ongoing interest in privacy encourages businesses to consider more carefully any changes in data collection or use that may make consumers feel uncomfortable about the safety and security of customer information.

That being said, we would encourage the Committee to re-evaluate the breadth of the proposed federal privacy legislation and focus more keenly on specific practices that may cause real consumer harm. As drafted, the scope of proposed legislation focuses on an enormous swath of data and its uses, without narrowly focusing on the practices that the Committee might find most harmful to consumers. In December 2010, the FTC released its initial staff report on a proposed U.S. policy framework for the collection and use of consumer information. While the Commission has expressed its concern that the business community did not act quickly enough to implement its suggested best-practices to address the more narrow subject of online behavioral advertising practices, we have seen a great deal of activity in this area from both a technological and self-regulatory standpoint. This indicates that the FTC's more targeted efforts are having their intended effect, and this type of issue-by-issue approach, which focuses on specific consumer information uses, helps businesses harness important changes in technology that may need to be made in order to provide consumers a greater sense of privacy and security.

In crafting and considering federal privacy legislation, we strongly urge the Committee to continue to respect the importance of information to businesses, particularly those practicing retail business models that have not been the subject of consumer complaints driving current federal agency inquiries and proposed privacy legislation. Retailers must collect, use and store information about their own customers going forward—it is vital to their businesses—and we continue to believe that first-party marketing (or marketing to one's own customers) should be exempted from any new notice-and-choice regime that may be proposed in privacy legislation. Information about customers is the lifeblood of retail, and effective marketing could not occur without the ability for retailers to understand their own customers over time and cater to their evolving interests in products. When the Committee members consider that consumer spending accounts for roughly two-thirds of our economy, and, that we are on the cusp of an economic recovery, now is the time for retailers to reach out even more effectively to their customers to get them into stores and spending again. Legislation that has the unintended consequence of limiting such important customer communications may very likely have a corresponding negative impact on our economy at a time we can least afford it.

The CHAIRMAN. So ordered. I thank the Senator and now turn to Julie Brill, who is the Commissioner of the Federal Trade Commission, one of the commissioners; and Austin Schlick, who is General Counsel of the Federal Communications Commission; and Cameron Kerry, General Counsel, the Department of Commerce—three pretty good witnesses.

Ms. Brill, if you wish to proceed.

STATEMENT OF HON. JULIE BRILL, COMMISSIONER, FEDERAL TRADE COMMISSION

Ms. BRILL. Thank you, Chairman Rockefeller, and Ranking Member Hutchison and members of the Committee. I am Julie Brill, a Commissioner of the Federal Trade Commission. I appreciate the opportunity to present the Commission's testimony today.

Vast amounts of personal information about consumers are collected and used by many different types of businesses, employers,

retailers, advertisers, data brokers, lenders, insurance companies, and many more. Imagine a cash-strapped mother working as a substitute teacher and waiting for a permanent opening. She and her husband have mounting bills, so to tide them over between paychecks, she gets a payday loan.

She then goes to the drugstore and buys diapers and Children's Tylenol with her loyalty card. Soon after, in the mail, she gets coupons for diapers and Children's Motrin, and she receives an offer to refinance her mortgage on terms that seem too good to be true.

In the evening, the mom goes online to spend time on a social network site. While online, she notices she is receiving ads for toys and children's cough medicine, as well as more loan offers.

Could the drugstore and social networking site have sold information about our consumer's purchases and interests? Could the payday lender have sold information about her need for money to other lenders and lead generators, both online and offline, who are offering her loans? Could the fact that she is a new mom be sold to potential employers? The answer to all of these questions is yes.

Some of the things I've described can offer real benefits. The mom probably wants coupons for diapers. But the vast majority of consumers are completely unaware that their purchasing history, their particular financial situation, information about their health and other personal information is sold to data brokers, lead generators, lenders, insurance companies, potential employers, and others.

Most consumers are simply unaware of the data deluge about them being collected, sold, and used both online and offline. I am concerned about how consumers' privacy is impacted by these practices.

At the Federal Trade Commission, we are focused on solutions that provide consumers with more information and more choices about these practices while allowing industry to continue to innovate and thrive. The FTC enforces laws protecting consumer privacy and security, educates consumers and businesses, and engages in policy initiatives.

Our written testimony highlights our many recent significant enforcement efforts related to privacy and data security, including our latest action announced just this week against Teletrack, a company that sold lists about financially distressed consumers to marketers. To settle our allegations, Teletrack agreed to comply with the Fair Credit Reporting Act and pay a $1.8 million civil penalty.

Privacy and security continue to be front and center on the Commission's policy agenda as well. The Commission has not taken a position on whether general privacy or do-not-track legislation is needed. But a majority of commissioners, myself included, supports widespread implementation of do-not-track mechanisms.

More generally, the Commission supports strong privacy protections. Our preliminary staff privacy report recommended that industry build privacy protections into their products and services at the outset, simplify choices presented to consumers about privacy, and improve transparency relating to data collection and use.

On data security, the Commission supports the enactment of federal data security and breach notification legislation. I am pleased

that legislation proposed in this committee aims to accomplish all of these goals.

Thank you for your leadership on consumer privacy and data security. We look forward to continuing to work closely with you on these critical issues.

[The prepared statement of Ms. Brill follows:]

PREPARED STATEMENT OF HON. JULIE BRILL, COMMISSIONER, FEDERAL TRADE COMMISSION

I. Introduction

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee, I am Julie Brill, a Commissioner of the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's testimony on consumer privacy.

Privacy has been an important component of the Commission's consumer protection mission for 40 years.[2] During this time, the Commission's goal in the privacy arena has remained constant: to protect consumers' personal information and ensure that they have the confidence to take advantage of the many benefits offered by the dynamic and ever-changing marketplace. To meet this objective, the Commission has undertaken substantial efforts to promote privacy in the private sector through law enforcement, education, and policy initiatives. For example, since 2001, the Commission has brought 34 cases challenging the practices of companies that failed to adequately protect consumers' personal information; more than 100 spam and spyware cases; and 16 cases for violation of the Children's Online Privacy Protection Act ("COPPA").[3] The Commission also has distributed millions of copies of educational materials for consumers and businesses to address ongoing threats to security and privacy. And the FTC examines the implications of new technologies and business practices on consumer privacy through ongoing policy initiatives, such as a recent proposed privacy framework.

This testimony begins by describing some of the uses of consumer data that affect consumers' privacy in today's economy. It then offers an overview of the Commission's recent efforts in the enforcement, education, and policy areas. While the testimony does not offer views on general privacy legislation, the Commission encourages Congress to enact data security legislation that would: (1) impose data security standards on companies, and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach.[4]

II. Information Flows in the Current Marketplace

For today's consumer, understanding the complex transfers of personal information that occur in the offline and online marketplaces is a daunting task. Indeed, these information flows take place in almost every conceivable consumer interaction. For example, a consumer goes to work and provides sensitive information to her employer, such as her Social Security Number, to verify her employment eligibility, and bank account number, so that she can get paid. After work, she uses an application on her Smartphone to locate the closest ATM so that she can withdraw cash. She then visits her local grocery store and signs up for a loyalty card to get dis-

---

[1] The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any other Commissioner. Commissioner William E. Kovacic dissents from this testimony to the extent that it endorses a Do Not Track mechanism. Commissioner Rosch dissents to the portions of the testimony that discuss and describe certain conclusions about the concept of Do Not Track. His views are included in an attached Separate Statement.

[2] Information on the FTC's privacy initiatives generally may be found at *business.ftc.gov/privacy-and-security*.

[3] 15 U.S.C. §§ 6501–6508.

[4] The Commission has long supported data security and breach notification legislation. See, *e.g.,* Prepared Statement of the Federal Trade Commission, *Data Security*, Before the Subcomm. on Commerce, Manufacturing, and Trade of the H. Comm. on Energy and Commerce, 112th Cong., June 15, 2011, available at *http://www.ftc.gov/os/testimony/110615datasecurity house.pdf* (noting the Commission's support for data security and breach notification standards); Prepared Statement of the Federal Trade Commission, *Protecting Social Security Numbers From Identity Theft*, Before the Subcomm. on Social Security of the H. Comm. on Ways and Means, 112th Cong., April 13, 2011, available at *http://ftc.gov/os/testimony/110411ssn-idtheft.pdf* (same); FTC, Security in Numbers, SSNs and ID Theft (Dec. 2008), available at *www.ftc.gov/os/2008/12/P075414ssnreport.pdf*; President's Identity Theft Task Force, Identity Theft Task Force Report (Sept. 2008), available at *http://www.idtheft.gov/reports/IDTReport2008.pdf*.

counts on future purchases. Upon returning home, the consumer logs onto her computer and begins browsing the web and updating her social networking page. Later, her child logs on to play an online interactive game.

All of these activities clearly benefit the consumer—she gets paid, enjoys free and immediate access to information, locates places of interest, obtains discounts on purchases, stays connected with friends, and can entertain herself and her family. Her life is made easier in a myriad of ways because of information flows.

There are other implications, however, that may be less obvious. Her grocery store purchase history, web activities, and even her location information, may be collected and then sold to data brokers and other companies she does not know exist. These companies could use her information to market other products and services to her or to make decisions about her eligibility for credit, employment, or insurance. And the companies with whom she and her family interact may not maintain reasonable safeguards to protect the data they have collected.

Some consumers have no idea that this type of information collection and sharing is taking place. Others may be troubled by the collection and sharing described above. Still others may be aware of this collection and use of their personal information but view it as a worthwhile trade-off for innovative products and services, convenience, and personalization. And some consumers—some teens for example—may be aware of the sharing that takes place, but may not appreciate the risks it poses. Because of these differences in consumer understanding, and attitudes, as well as the rapid pace of change in technology, policymaking on privacy issues presents significant challenges and opportunities.

As the hypothetical described above shows, consumer privacy issues touch many aspects of our lives in both the brick-and-mortar and electronic worlds. In the offline world, data brokers have long gathered information about our retail purchases, and consumer reporting agencies have long made decisions about our eligibility for credit, employment, and insurance based on our past transactions. But new online business models such as online behavioral advertising, social networking, interactive gaming, and location-based services have complicated the privacy picture. In addition, the aggregation of data in both the online and offline worlds have in some instances led to increased opportunities for fraud. For instance, entities have used past transaction history gathered from both the online and offline world to sell "sucker lists" of consumers who may be susceptible to different types of fraud. In both the online and offline worlds, data security continues to be an issue. The FTC continues to tackle each of these issues through enforcement, education, and policy initiatives.

III. Enforcement

In the last 15 years, the Commission has brought 34 data security cases; 64 cases against companies for improperly calling consumers on the Do Not Call registry;[5] 86 cases against companies for violating the Fair Credit Reporting Act ("FCRA");[6] 97 spam cases; 15 spyware (or nuisance adware) cases; and 16 cases against companies for violating COPPA. Where the FTC has authority to seek civil penalties, it has aggressively done so. It has obtained $60 million in civil penalties in Do Not Call cases; $21 million in civil penalties under the FCRA; $5.7 million under the CAN–SPAM Act;[7] and $6.2 million under COPPA. Where the Commission does not have authority to seek civil penalties, as in the data security and spyware areas, it has sought such authority from Congress. In addition, the Commission has brought numerous cases against companies for violating the FTC Act by making deceptive claims about the privacy protection they afford to the information they collect. And these numbers do not fully reflect the scope of the Commission's vigorous enforcement agenda, as not all investigations result in enforcement actions. When an enforcement action is not warranted, staff closes the investigation, and in some cases it issues a closing letter."[8] This testimony highlights the Commission's recent, publicly-announced enforcement efforts to address the types of privacy issues raised by the hypothetical scenario described above.

First, the Commission enforces the FTC Act and several other laws that require companies to maintain reasonable safeguards for the consumer data they maintain.[9]

---

[5] 16 C.F.R. Part 310.
[6] 15 U.S.C. §§ 1681e–i.
[7] 15 U.S.C. §§ 7701–7713.
[8] *See http://www.ftc.gov/os/closings/staffclosing.shtm*.
[9] *See* the Commission's Safeguards Rule under the Gramm-Leach-Bliley Act, 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b), and provisions of the FCRA, 15 U.S.C. §§ 1681e, 1681w, implemented at 16 C.F.R. Part 682.

Most recently, the Commission resolved allegations that Ceridian Corporation [10] and Lookout Services, Inc.[11] violated the FTC Act by failing to implement reasonable safeguards to protect the sensitive consumer information they maintained. The companies offered, respectively, payroll processing and immigration compliance services for small business employers. As a result, they both obtained, processed, and stored highly-sensitive information—including Social Security numbers—of employees. The Commission alleged that both companies failed to appropriately safeguard this information, which resulted in intruders being able to access it. The orders require the companies to implement a comprehensive data security program and obtain independent audits for 20 years.

Second, the Commission enforces the FCRA, which, among other things, prescribes that companies only sell sensitive consumer report information for "permissible purposes," and not for general marketing purposes. Just this week, the Commission announced an FCRA enforcement action against Teletrack for violating this provision. Teletrack provides consumer reporting services to payday lenders, rental purchase stores, and certain auto lenders, so that they can determine consumers' eligibility to receive credit.[12] The Commission alleged that Teletrack created a marketing database of consumers, and sold lists of consumers who had applied for payday loans to entities that did not have a permissible purpose. The Commission asserted that Teletrack's sale of these lists violated the FCRA because the lists were in fact consumer reports, which cannot be sold for marketing purposes. The Commission's agreement with Teletrack requires it to pay $1.8 million in civil penalties for FCRA violations.

Third, the Commission has been active in ensuring that companies engaged in social networking adhere to any promises to keep consumers' information private.[13] The Commission's recent case against Google alleges that the company deceived consumers by using information collected from Gmail users to generate and populate its new social network, Google Buzz.[14] The Commission charged that Google made public its Gmail users' associations with their frequent e-mail contacts without the users' consent and in contravention of Google's privacy policy. As part of the Commission's proposed settlement order, Google must implement a comprehensive privacy program and conduct independent audits every other year for the next 20 years.[15] Further, Google must obtain affirmative express consent for product or service enhancements that involve new sharing of previously collected data.

Fourth, the Commission has sought to protect consumers from deceptive practices in the behavioral advertising area. In June, the Commission finalized a settlement with Chitika, Inc., an online network advertiser that acts as an intermediary between website publishers and advertisers.[16] The Commission's complaint alleged that Chitika violated the FTC Act by offering consumers the ability to opt out of the collection of information to be used for targeted advertising—without telling them that the opt-out lasted only 10 days. The Commission's order prohibits Chitika from making future privacy misrepresentations. It also requires Chitika to provide consumers with an effective opt-out mechanism, link to this opt-out mechanism in its advertisements, and provide a notice on its website for consumers who may have opted out when Chitika's opt-out mechanism was ineffective. Finally, the order requires Chitika to destroy any data that can be associated with a consumer that it collected during the time its opt-out mechanism was ineffective.

Fifth, the Commission has tried to ensure that data brokers respect consumers' choices. In March, the Commission announced a final order against U.S. Search, a data broker that maintained an online service, which allowed consumers to search

---

[10] *Ceridian Corp.*, FTC Docket No. C–4325 (June 8, 2011) (consent order), available at *www.ftc.gov/opa/2011/05/ceridianlookout.shtm*.

[11] *Lookout Servs., Inc.,* FTC Docket No. C–4326 (June 15, 2011) (consent order), available at *www.ftc.gov/opa/2011/05/ceridianlookout.shtm*.

[12] *See U.S.* v. *Teletrack, Inc.*, No. 1:11–CV–2060 (N.D. Ga. filed June 24, 2011) (proposed consent order), available at *http://www.ftc.gov/opa/2011/06/teletrack.shtm*.

[13] *See, e.g., Twitter, Inc.,* FTC Docket No. C–4316 (Mar. 2, 2011) (consent order), available at *http://www.ftc.gov/opa/2010/06/twitter.shtm* (resolving allegations that social networking service Twitter deceived its customers by failing to honor their choices after offering the opportunity to designate certain "tweets" as private).

[14] *Google, Inc.*, FTC File No. 102 3136 (Mar. 30, 2011) (consent order accepted for public comment), available at *www.ftc.gov/opa/2011/03/google.shtm*. Commissioner Rosch issued a concurring statement expressing concerns about the terms of the proposed consent agreement, available at *http://www.ftc.gov/os/caselist/1023136/110330googlebuzzstatement.pdf*.

[15] This provision would apply to any data collected by Google about users of any Google product or service, including mobile and location-based data.

[16] *Chitika, Inc.*, FTC Docket No. C–4324 (June 7, 2011) (consent order), available at *http://www.ftc.gov/opa/2011/03/chitika.shtm*.

for information about others.[17] The company allowed consumers to opt out of having their information appear in search results, for a fee of $10. The Commission charged that although 4,000 consumers paid the fee and opted out, their personal information still appeared in search results. The Commission's settlement requires U.S. Search to disclose limitations on its opt-out offer, and to provide refunds to consumers who had previously opted out.

Finally, to protect children's privacy, the Commission enforces the Children's Online Privacy Protection Act ("COPPA"). In its most recent case, against Playdom, Inc. and one of its senior executives, the Commission obtained an agreement with the operators of 20 online virtual worlds to pay $3 million to settle charges that they violated COPPA by illegally collecting and disclosing personal information from hundreds of thousands of children under age 13 without their parents' consent.[18] The defendants allegedly collected children's ages and e-mail addresses during registration and then enabled them to publicly post their full names, e-mail addresses, instant messenger IDs, and location on personal profile pages and in online community forums. The FTC charged that the defendants' failure to provide proper notice or obtain parents' prior verifiable consent before collecting or disclosing children's personal information violated COPPA. It further charged that the defendants violated the FTC Act because their privacy policy misrepresented that the company would prohibit children under 13 from posting personal information online. In addition to the $3 million civil penalty—the largest ever for a COPPA violation—the proposed settlement permanently bars the defendants from violating COPPA and from misrepresenting their information practices regarding children.

IV. Education

The FTC conducts outreach to businesses and consumers in the area of consumer privacy. The Commission's well-known OnGuard Online website educates consumers about many online threats to consumer privacy and security, including spam, spyware, phishing, peerto-peer ("P2P") file sharing, and social networking.[19] The Commission has also issued numerous education materials to help consumers protect themselves from identity theft and to deal with its consequences when it does occur. The FTC has distributed over 3.8 million copies of a victim recovery guide—*Take Charge: Fighting Back Against Identity Theft*—and has recorded over 3.5 million visits to the Web version. In addition, the FTC has developed education resources specifically for children, parents, and teachers to help children stay safe online. In response to the Broadband Data Improvement Act of 2008, the FTC produced the brochure *Net Cetera: Chatting with Kids About Being Online* to give adults practical tips to help children navigate the online world.[20] In less than 1 year, the Commission distributed more than 7 million copies of Net Cetera to schools and communities nationwide.

Business education is also an important priority for the FTC. The Commission developed a widely-distributed guide to help small and medium-sized businesses implement appropriate data security for the personal information they collect and maintain.[21]

Another way in which the Commission seeks to educate businesses is by publicizing its complaints and orders and issuing public closing letters. For example, the Commission recently sent a letter closing an investigation of Social Intelligence Corporation, a company that sold reports to employers about potential job applicants.[22] The reports included public information gathered from social networking sites. The investigation sought to determine Social Intelligence's compliance with the FCRA.[23] Although the staff decided to close the particular investigation, the public closing letter served to notify similarly situated businesses that, to the extent they collect information from social networking sites for employment determinations, they must comply with the FCRA. The letter included guidance on the obligations of such busi-

---

[17] *US Search, Inc.*, FTC Docket No. C–4317 (Mar. 14, 2011) (consent order), available at *http://www.ftc.gov/opa/2010/09/ussearch.shtm*.

[18] *See U.S.* v. *Playdom, Inc.*, No. SACV11–00724 (C.D. Cal. filed May 11, 2011) (proposed consent order), available at *http://www.ftc.gov/opa/2011/05/playdom.shtm*.

[19] *See www.onguardonline.gov*. Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alertaena Lϕnea have attracted nearly 12 million unique visits.

[20] *See* Press Release, FTC, OnGuardOnline.gov Off to a Fast Start with Online Child Safety Campaign (Mar. 31, 2010), available at *www.ftc.gov/opa/2010/03/netcetera.shtm*.

[21] *See Protecting Personal Information: A Guide For Business*, available at *www.ftc.gov/infosecurity*.

[22] Letter from Maneesha Mithal, Associate Director, Division of Privacy and Identity Protection to Renee Jackson, Counsel to Social Intelligence Corporation (May 9, 2011), available at *www.ftc.gov/os/closings/110509socialintelligenceletter.pdf*.

[23] FTC staff did not express an opinion on the merits of Social Intelligence's business model.

nesses under the FCRA. For example, companies must take reasonable steps to ensure the maximum possible accuracy of the information reported from social networking sites. They must also provide employers who use their reports with information about the employers' obligation to notify job applicants if they were denied employment on the basis of these reports, and to provide such applicants with information about their rights under the FCRA.

V. Policy Initiatives

The Commission's privacy program also includes public workshops, reports, and policy reviews to examine the implications of new technologies and business practices on consumer privacy. For example, in December 2009, February 2010, and March 2010, the FTC convened three public roundtables to explore consumer privacy issues, including the issues facing the hypothetical consumer discussed in Section II above.[24]

Based on these roundtable discussions, staff issued a preliminary report in December 2010,[25] which proposed and solicited comment on a new framework to guide policymakers and industry as they consider further steps to improve consumer privacy protection. The proposed framework included three main concepts.

First, staff recommended that companies should adopt a "privacy by design" approach by building privacy protections into their everyday business practices, such as collecting or retaining only the data they need to provide a requested service or transaction, and implementing reasonable security for such data. Thus, for example, if a mobile application ("app") is providing traffic and weather information to a consumer, it does need to collect call logs or contact lists from the consumer's device. Similarly, if an app does need sensitive information, such as location, in order to provide a requested service, the app developer should carefully consider how long the information should be retained to provide such service and how the information should best be protected.

Second, staff proposed that companies provide simpler and more streamlined choices to consumers about their data practices. One example of how choice may be simplified for consumers is through a universal, one-stop choice mechanism for online behavioral tracking, often referred to as "Do Not Track." The Staff Report recommended implementation of such a system.[26] Following the release of the Staff Report, the Commission has testified that any Do Not Track system should include certain attributes.[27] First, any Do Not Track system should be implemented universally, so that consumers do not have to repeatedly opt out of tracking on different sites. Second, the choice mechanism should be easy to find, easy to understand, and easy to use. Third, any choices offered should be persistent and should not be deleted if, for example, consumers clear their cookies or update their browsers. Fourth, a Do Not Track system should be comprehensive, effective, and enforceable. It should opt consumers out of behavioral tracking through any means and not permit technical loopholes. Finally, an effective Do Not Track system would go beyond simply opting consumers out of receiving targeted advertisements; it would opt them

---

[24] *See generally* FTC Exploring Privacy web page, at *www.ftc.gov/bcp/workshops/privacyroundtables*.

[25] *See A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010), available at *www.ftc.gov/os/2010/12/101201privacyreport.pdf*. Commissioners Kovacic and Rosch issued concurring statements available at *www.ftc.gov/os/2010/12/101201privacyreport.pdf* at Appendix D and Appendix E, respectively.

[26] Commissioner Kovacic believes that the endorsement of a Do Not Track mechanism by staff (in the report) and the Commission (in this testimony) is premature. His concerns about the Commission Staff Report are set forth in his statement on the report. *See* FTC Staff Report, *supra* note 22, at App. D. Commissioner Rosch supported a Do Not Track mechanism only if it were "technically feasible" and implemented in a fashion that provides informed consumer choice regarding all the attributes of such a mechanism. *Id.* At App. E. Commissioner Rosch continues to believe that a variety of issues need to be addressed prior to the endorsement of any particular Do Not Track mechanism. *See* Statement of Commissioner J. Thomas Rosch, Dissenting in Part, *Privacy and Data Security: Protecting Consumers in the Modern World*, Hearing Before the S. Comm. on Commerce, Science, and Transportation, 112th Cong. (June 29, 2011).

[27] *See, e.g.,* Prepared Statement of the Federal Trade Commission, *The State of Online Consumer Privacy*, Hearing Before the S. Comm. on Commerce, Science and Transportation, 112th Cong. (Mar. 16, 2011), available at *http://www.ftc.gov/os/testimony/110316consumerprivacysenate.pdf*; Prepared Statement of the Federal Trade Commission, Do Not Track, Hearing Before the Subcomm. on Commerce, Trade and Consumer Protection of the H. Comm. on Energy and Commerce, 111th Cong. (Dec. 2, 2010), available at *www.ftc.gov/os/testimony/101202donottrack.pdf* (hereinafter "Do Not Track Testimony").

out of collection of behavioral data for all purposes other than product and service fulfillment and other commonly accepted practices.[28]

Of course, any Do Not Track system should not undermine the benefits that online behavioral advertising has to offer, by funding online content and services and providing personalized advertisements that many consumers value. For this reason, any Do Not Track mechanism should be flexible. For example, it should allow companies to explain the benefits of tracking and to take the opportunity to convince consumers not to opt out of tracking. Further, a Do Not Track system could include an option that enables consumers to control the types of advertising they want to receive and the types of data they are willing to have collected about them, in addition to providing the option to opt-out completely.[29]

Industry appears to be receptive to the demand for simple choices. Recently, three of the major browsers offered by Mozilla, Microsoft, and Apple, announced the development of new choice mechanisms for online behavioral advertising that seek to provide increased transparency, greater consumer control and improved ease of use. More recently, Mozilla introduced a version of its browser that enables Do Not Track for mobile web browsing. In addition, an industry coalition of media and marketing associations, the Digital Advertising Alliance, has continued to make progress on implementation of its improved disclosure and consumer choice mechanism offered through a behavioral advertising icon.

Third, the Staff Report proposed a number of measures that companies should take to make their data practices more transparent to consumers. For instance, in addition to providing the contextual disclosures described above, companies should improve their privacy notices so that consumers, advocacy groups, regulators, and others can compare data practices and choices across companies, thus promoting competition among companies. The staff also proposed providing consumers with reasonable access to the data that companies maintain about them, particularly for non-consumer-facing entities such as data brokers. Because of the significant costs associated with access, the Staff Report noted that the extent of access should be proportional to both the sensitivity of the data and its intended use. Staff is evaluating the 450 comments received and expects to issue a final report later this year.

In addition to issuing reports, the Commission also reviews its rules periodically to ensure that they keep pace with changes in the marketplace. The Commission is currently reviewing its rule implementing COPPA and anticipates that any proposed changes will be announced in the coming months.[30]

Finally, the Commission hosts workshops to study and publicize more specific issues. One such issue that has been in the news recently is identity theft targeting children.[31] For a variety of reasons—including poor safeguards for protecting children's data—identity thieves can get access to children's Social Security numbers. These criminals may deliberately use a child's Social Security number, or fabricate a Social Security number that coincidentally has been assigned to a child, in order to obtain employment, apply for government benefits, open new accounts, or apply for car loans or even mortgages. Child identity theft is especially pernicious because the theft may not be detected until the child becomes an adult and seeks employment, or applies for student and car loans.

To address the challenges raised by child identity theft, Commission staff, along with the Department of Justice's Office of Victims of Crime, will host a forum on July 12, 2011.[32] Participants will include educators, child advocates, and representatives of various governmental agencies and the private sector. The forum will include a discussion on how to improve the security of children's data in various contexts—including within the education system as well as the foster care system—where children may be particularly susceptible to identity theft. The goal of the

---

[28] As noted in prior Commission testimony, such a mechanism should be different from the Do Not Call program in that it should not require the creation of a "Registry" of unique identifiers, which could itself cause privacy concerns. See Do Not Track Testimony, *supra* note 27.

[29] For example, use of a Do Not Track browser header would enable consumer customization. The browser could send the header to some sites and not others. Moreover, a particular site could ignore the header to the extent the user has consented to tracking on that site.

[30] *See generally* COPPA Rulemaking and Rule Reviews web page, available at *business.ftc.gov/documents/coppa-rulemaking-and-rule-reviews*.

[31] *See, e.g.,* Richard Power, Carnegie Mellon Cylab, *Child Identity Theft, New Evidence Indicates Identity Thieves are Targeting Children for Unused Social Security Numbers* (2011), available at *www.cyblog.cylab.cmu.edu/2011/03/child-identity-theft.html*; Children's Advocacy Institute, *The Fleecing of Foster Children: How We Confiscate Their Assets and Undermine Their Financial Security* (2011), available at *http://www.caichildlaw.org/Misc/Fleecing__Report__Final__HR.pdf*.

[32] *See* Press Release, FTC, Department of Justice to Host Forum on Child Identity Theft (June 2, 2011), available at *www.ftc.gov/opa/2011/06/childtheft.shtm*.

forum is to develop ways to effectively advise parents on how to avoid child identity theft, how to protect children's personal data, and how to help parents and young adults who have been victims of child identity theft recover from the crime.

VI. Conclusion

The Commission is committed to protecting consumers' privacy and security—both online and offline. We look forward to continuing to work with Congress on these critical issues.

ATTACHMENT

PREPARED STATEMENT OF COMMISSIONER J. THOMAS ROSCH, DISSENTING IN PART
PRIVACY AND DATA SECURITY: PROTECTING CONSUMERS IN THE MODERN WORLD

The root problem with the concept of "Do Not Track" is that we, and with respect, the Congress, do not know enough about most tracking to determine how to achieve the five attributes identified in today's Commission testimony, or even whether those attributes can be achieved.[1] Considered in a vacuum, the proposed Do Not Track attributes set forth in today's testimony can be considered innocuous, indeed even beneficial. However, the concept of Do Not Track cannot be considered in a vacuum. The promulgation of five attributes, standing alone, untethered to actual business practices and consumer preferences, and not evaluated in light of their impact upon innovation or the Internet economy, is irresponsible. I therefore respectfully dissent to the portions of the testimony that discuss and describe certain conclusions about the concept of Do Not Track.[2]

It is easy to attack practices that threaten data security. There is a consensus in both the United States and Europe that those practices are pernicious, and the Commission has successfully challenged them.[3] It is also easy to attack practices that compromise certain personally identifiable information ("PII") like one's social security number, confidential financial or health data, or other sensitive information, such as that respecting children. The consensus about those practices in the United States is reflected in federal statutes like the Health Insurance Portability and Accountability Act ("HIPAA"), the Gramm-Leach-Bliley Act ("GLBA"), and the Children's Online Privacy Protection Act ("COPPA"), and the Commission has likewise successfully challenged practices that violate those statutes.[4] On the other hand, some of the "tracking" that occurs routinely is benign, such as tracking to ensure against advertisement repetition and other tracking activities that are essential to ensuring the smooth operation of websites and Internet browsing. But we do not know enough about other kinds of "tracking"—or what consumers think about

---

[1] As described in today's and prior testimony, the five attributes are:
First, any Do Not Track system should be implemented universally, so that consumers do not have to repeatedly opt out of tracking on different sites. Second, the choice mechanism should be easy to find, easy to understand, and easy to use. Third, any choices offered should be persistent and should not be deleted if, for example, consumers clear their cookies or update their browsers. Fourth, a Do Not Track system should be comprehensive, effective, and enforceable. It should opt consumers out of behavioral tracking through any means and not permit technical loopholes. Finally, an effective Do Not Track system would go beyond simply opting consumers out of receiving targeted advertisements; it would opt them out of collection of behavioral data for all purposes other than product and service fulfillment and other commonly accepted practices.

[2] The concept of Do Not Track was presented in the preliminary Staff Privacy Report, issued in December 2010. *See http://www.ftc.gov/os/2010/12/101201privacyreport.pdf*. At that time, the Commission requested public comment on the issues raised in that preliminary report.

[3] *See, e.g., Lookout Servs., Inc.*, FTC File No. 1023076 (June 15, 2011) (consent order) (alleging failure to reasonably and appropriately secure employees' and customers' personal information, collected and maintained in an online data base); *CVS Caremark Corp.*, FTC File No. 0723119 (June 18, 2009) (consent order) (alleging failure to implement reasonable policies and procedures for secure disposal of personal information); *BJ's Wholesale Club, Inc.*, FTC Docket No. C–4148 (Sept. 20, 2005) (consent order) (alleging failure to take reasonable and appropriate security measures to protect sensitive consumer financial information with respect to credit and debit card purchases); *Eli Lilly and Co.*, FTC File No. 0123214 (May 8, 2002) (consent order) (alleging failure to provide appropriate training for employees regarding consumer privacy and information security).

[4] *Rite Aid Corp.*, FTC File No. 0723121 (Nov. 12, 2010) (consent order) (in conjunction with HHS; alleging failure to establish policies and procedures for the secure disposal of consumers' sensitive health information) (HIPAA); *SettlementOne Credit Corp.*, FTC File No. 0823208 (Feb. 9, 2011) (proposed consent agreement) (alleging that credit report reseller failed to implement reasonable safeguards to control risks to sensitive consumer information) (GLBA); *United States v. Playdom, Inc.*, Case No. SACV 11–0724–AG(ANx) (C.D. Cal. May 24, 2011) (consent order) (alleging failure to provide notice and obtain consent from parents before collecting, using, and disclosing children's personal information) (COPPA).

it—to reach any conclusions about whether most consumers consider it good, bad or are indifferent.

More specifically, it is premature to endorse any particular browser's Do Not Track mechanism. One type of browser mechanism proposed to implement Do Not Track involves the use of "white lists" and "black lists" to allow consumers to pick and choose which advertising networks they will allow to track them.[5] These lists are furnished by interested third parties in order to prevent the types of tracking that consumers supposedly do not want.[6] It is clear from these "lists" what the interested third parties think about the tracking on the lists (or not on the lists). However, it is not clear whether most consumers share those views, or even understand the basis upon which the "list" was created. Another proposed browser Do Not Track mechanism operates by sending a Do Not Track header as consumers surf the Internet. This mechanism would only eliminate tracking to the extent that the entities receiving the Do Not Track header understand and respect that choice. Theoretically at least, this mechanism could block all tracking if it does not offer customization and preserve the ability to customize.[7] This is important because there may be some tracking that consumers find beneficial and wish to retain.

Beyond that, consumers (including consumers that are surveyed by interested third parties) are generally not fully informed about the consequences—both bad and good—of subscribing to a Do Not Track mechanism.[8] They are not always told, for example, that they may lose content (including advertising) that is most pertinent and relevant to them. Neither are they told that they may lose free content (that is paid for by advertising). Nor are they told that subscribing to a Do Not Track mechanism may result in more obtrusive advertising or in the loss of the chance to "sell" the history of their Internet activity to interested third parties. Indeed, they are not even generally told what kinds of tracking are going to be eliminated. On the other hand, consumers are not told that tracking may facilitate the compilation of a consumer "profile" through the aggregation of information by third parties to whom it is sold or with whom it is shared (such as insurance companies engaged in "rating" consumers). One reason that consumers are not told about the latter consequence is that we do not know enough about what information is being collected and sold to third parties to know the extent to which such aggregation is occurring.

One thing is certain though: consumers cannot expect simply to "register" for a Do Not Track mechanism as they now register for "Do Not Call."[9] That is because a consumer registering for Do Not Call needs to furnish only his or her phone number. In the context of the Do Not Call program, each telephone already has a unique identifier in the form of a telephone number. In contrast, there is no such persistent identifier for computers. For example, Internet Protocol ("IP") addresses can and do change frequently. In this context, creating a persistent identifier, and then submitting it to a centralized data base, would raise significant privacy issues.[10] Thus, information respecting the particular computer involved is essential, and that kind of information cannot be furnished without compromising the very confidential information that consumers supposedly do not want to share. In addition, multiple users of the same computer or device may have different preferences, and tying a broad Do Not Track mechanism to a particular computer or device does not take that into consideration.

This is not to say that a Do Not Track mechanism is not feasible. It is to say that we must gather competent and reliable evidence about what kind of tracking is occurring before we embrace any particular mechanism. We must also gather reliable evidence about the practices most consumers are concerned about. Nor is it to

---

[5] Many, if not all, browsers currently allow consumers to customize their browser to prevent the installation of, or delete already installed, cookies that are used for tracking.

[6] Some Tracking Protection Lists (TPLs) allow any criterion to be used to decide which sites go on a TPL and which do not. In some cases, consumers may have the option to create their own TPL. However, as discussed below, neither the FTC, nor consumer advocates, nor consumers themselves, know enough about the tracking, collection, retention and sharing practices of online entities.

[7] In addition, it is not clear how the "recipient" of the Do Not Track header would respond to such a request when the consumer has otherwise indicated that he or she wishes to have the recipient customize the consumer's experience.

[8] That is not to say that current technology cannot facilitate these disclosures. However, it is critical that advertisers and publishers take the opportunity to explain to consumers what their practices are and why they might be beneficial.

[9] *See* Prepared Statement of the Federal Trade Commission on Do Not Track Before the House Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection, Dec. 2, 2010, available at *http://www.ftc.gov/os/testimony/101202donottrack.pdf*.

[10] A new identifier would be yet another piece of PII that companies could use to gather data about individual consumers.

say that it is impossible to gather that evidence. The Commission currently knows the identities of several hundred ad networks representing more than 90 percent of those entities engaged in the gathering and sharing of tracking information. It is possible to serve those networks with compulsory process, which means that the questions about their information practices (collection, tracking, retention and sharing) must be answered under oath. That would enable the Commission to determine and report the kinds of information practices that are most frequently occurring. Consumers could then access more complete and reliable information about the consequences of information collection, tracking, retention and sharing. Additionally, the Commission could either furnish, or, depending on technical changes that may occur, facilitate the furnishing of, more complete and accurate "lists" and consumers would then have the ability to make informed choices about the collection, tracking, retention and sharing practices they would or would not permit.

This course is not perfect. For one thing, it would take time to gather this information. For another thing, it would involve some expense and burden for responding parties (though no more than that to which food and alcohol advertisers who currently must answer such questionnaires are exposed). Consumers would also be obliged to avail themselves of the information provided by the Commission. But I respectfully submit that this course is superior to acting blindly, which is what I fear we are doing now.

The CHAIRMAN. Thank you, Ms. Brill.

Welcome, Mr. Kerry.

STATEMENT OF HON. CAMERON F. KERRY, GENERAL COUNSEL, U.S. DEPARTMENT OF COMMERCE

Mr. KERRY. Thank you. Thank you, Chairman Rockefeller, Senator Thune, and members of the Committee. I welcome the opportunity to be here today and to discuss with you the issue of how we can best protect consumer data privacy in a digital age. This is an issue that affects everyone.

At this committee's hearing on March 16, the Obama Administration urged legislation to establish basic commercial data privacy protection for all U.S. consumers. What we recommended then had three elements.

The first is baseline privacy protection in the form of a consumer privacy bill of rights adapted from widely accepted fair information practice principles. The second is for government to convene multistakeholder processes to encourage the private sector to develop legally enforceable, context specific codes of conduct that implement the bill of rights in specific context.

And the third is to bolster the Federal Trade Commission's leadership in this field by granting it explicit authority to enforce the privacy bill of rights and to grant safe harbors for revolving codes of conduct.

We are encouraged that members of this committee and others in Congress have introduced several bills to address significant data privacy issues. The Administration looks forward to working closely with members of this committee and Congress to pass legislation that will protect consumer interests and provide businesses and consumers with a clear and consistent set of rules of the road both within the United States and internationally.

Our conclusion that the time has come for comprehensive data privacy protection is a product of the work of the Department of Commerce Internet Policy Task Force and the National Science and Technology Council subcommittee that I co-chair. It reflects two tenets.

The first is very simply that to harness the full power of the Internet, we need clear rules that allow for innovation and economic growth while protecting trust and respecting consumers' legitimate privacy expectations. Consumer groups, industry, and leading privacy scholars agree that a large percentage of Americans do not know what information is being collected about them or how they can control collection and use.

Second, as we establish guidelines, we need to avoid a regulatory environment that restricts the innovation and the free flow of information that have been hallmarks of the Internet and drivers of economic growth and an expansion of information that stretches the boundaries of human knowledge and creates social and political change. Legislation shouldn't add duplicative or overly burdensome regulatory requirements to businesses that already adhere to strong privacy principles or that are subject to existing sectoral regimes. Legislation should be technology neutral so that, consistent with baseline principles, firms have flexibility to adapt technology to comply and to adopt business models that use data in ways not contemplated today.

Our work continues as the Administration finishes a white paper on commercial privacy. At the Department of Commerce, we will engage with stakeholders on the development of codes of conduct. We will work on data security and work with other agencies to ensure global interoperability.

This is an area where Congressional action can have significant impact. Two weeks ago, I was in Budapest to speak with European data privacy commissioners. And I can report to you that comprehensive legislation will send a strong message of U.S. leadership that could form a model for our partners, help prevent fragmentation of the world's privacy laws, and undo restrictions on businesses that conduct international trade.

So, Mr. Chairman, we look forward to working with you, the Committee, stakeholders, the FTC, and with other federal agencies toward enactment of legislation in the field. I ask that my written comments be included in the record and welcome any questions.

Thank you again for this opportunity.

[The prepared statement of Mr. Kerry follows:]

PREPARED STATEMENT OF HON. CAMERON F. KERRY, GENERAL COUNSEL, U.S. DEPARTMENT OF COMMERCE

I. Introduction

Chairman Rockefeller, Ranking Member Hutchison, and distinguished Committee members, thank you for the opportunity to testify about the important issue of online privacy on behalf of the Department of Commerce ("Department" or "Commerce"). I welcome the opportunity to discuss how we can best protect consumer data privacy in the Digital Age. And I am pleased to testify here today with Commissioner Julie Brill of the Federal Trade Commission (FTC) and a fellow General Counsel, Austin Schlick of the Federal Communications Commission (FCC).

At this committee's March 16, 2011, hearing on "The State of Online Data Privacy," the Administration announced its support for legislation that would create baseline consumer data privacy protections through a "consumer privacy bill of rights."[1] We urged Congress to consider legislation that would establish these rights

[1] Statement of Lawrence E. Strickling, Assistant Secretary for Communications and Information, before the Committee on Commerce, Science, and Transportation, U.S. Senate, Mar. 16, 2011, *http://www.ntia.doc.gov/presentations/2011/Strickling_Senate_Privacy_Testimony_03162011.html*.

and obligations; to encourage the private sector to develop legally-enforceable, industry-specific codes of conduct that can address emerging privacy issues while providing companies some assurance that they are in compliance with the law; and to grant the FTC the proper authority to enforce the law.

We are encouraged that members of this committee and others have introduced several bills that reflect a bipartisan effort to address significant consumer data privacy issues affecting our society and our economy.

Since this committee's hearing in March, we have been hard at work fleshing out Administration views on the issues we highlighted then. These views will inform an Obama Administration "White Paper" on consumer data privacy, which we are in the midst of drafting. I am here today to say we look forward to working with this Committee and other Members of Congress to pass legislation that will protect consumers' interests and provide businesses clear and consistent rules of the road.

As we stated in March, the Administration supports legislation that, first, creates a set of basic privacy protections in the commercial context for all American consumers. Second, the Administration supports creating incentives for the private sector to develop legally-enforceable rules that specify how to implement this bill of rights in specific business contexts. Third, because enforcement is critical to ensuring that any consumer privacy bill of rights is effective, the Administration supports granting the FTC clear authority to enforce the privacy obligations established by legislation.[2]

I will outline briefly how we arrived at these premises, and then elaborate on each one.

II. The Need to Strengthen Our Consumer Data Privacy Framework

Strengthening consumer data privacy protections is integral to the Department's Internet policy agenda. Consumer data privacy is one of the core issues under assessment by the Department's Internet Policy Task Force, which Secretary Gary Locke convened to examine how well U.S. policies on privacy, cybersecurity, copyright protection, and the free flow of information serve consumers, businesses, and other participants in the Internet economy.[3]

The Internet economy has sparked tremendous innovation, and the Internet is an essential platform for economic growth, domestically and globally. Digital technology linked by the Internet has enabled large-scale collection, analysis, and storage of personal information. These tools enable new service options and capabilities but they also create risks to individual privacy.

Privacy is a key ingredient for sustaining consumer trust, which in turn is critical to realize the full potential for innovation and the growth of the Internet. The technical and organizational complexity of this environment makes it challenging for individual consumers to understand and manage the uses of their personal data even if they are technically adept.

The Commerce Internet Policy Task Force has engaged with a broad array of stakeholders, including companies, consumer advocates, academic privacy experts, and other government agencies. Our work produced the Task Force's "Green Paper" on consumer data privacy in the Internet economy on December 16, 2010.[4] The privacy Green Paper made ten separate recommendations on how to strengthen consumer data privacy protections while also promoting innovation, but it also brought to light many additional questions.

The comments we received on the privacy Green Paper from business, academics, and advocates informed our conclusion that the U.S. consumer data privacy framework will benefit from legislation that establishes a clearer set of rules for businesses and consumers, while preserving the innovation and free flow of information that are hallmarks of the Internet. This conclusion reflects two tenets. First, to harness the full power of the Internet, we need to establish norms and ground rules for uses of information that allow for innovation and economic growth while respecting consumers' legitimate privacy interests. Consumer groups, industry, and leading privacy scholars agree that a large percentage of Americans do not fully understand and appreciate what information is being collected about them, and how they are

---

[2] *Id.*

[3] U.S. Dept. of Commerce, Commerce Secretary Locke Announces Public Review of Privacy Policy and Innovation in the Internet Economy, Launches Internet Policy Task Force, Apr. 21, 2010, *http://www.commerce.gov/print/news/press-releases/2010/04/21/commerce-secretary-locke-announces-public-review-privacy-policy-and-i.*

[4] Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, Dec. 16, 2010, *http://www.ntia.doc.gov/reports/2010/IPTF__Privacy__GreenPaper__12162010.pdf.*

able to stop certain practices from taking place.[5] Second, as we go about establishing these privacy guidelines, we also need to be careful to avoid creating an overly complicated regulatory environment.[6]

III. Strengthening Our Consumer Data Privacy Framework Through Baseline Protections

To achieve these goals, the Administration recommended legislation to establish baseline consumer data privacy protections that will apply in commercial contexts and help fill in gaps in current privacy laws. These protections should be flexible, enforceable at law, and serve as the basis for both enforcement and development of enforceable codes of conduct that specify how the legislative principles apply in specific business contexts. Though we are still reviewing the details of the various bills introduced, we note they generally adopt an approach of defining baseline obligations for companies that handle personal data; giving the FTC enforcement authority; and encouraging the development of industry-specific codes of conduct to implement these baseline requirements.

A. Enacting a Consumer Privacy Bill of Rights

The Administration recommended that statutory baseline protections for consumer data privacy be enforceable at law and based on a comprehensive set of Fair Information Practice Principles (FIPPs). In the Department of Commerce Green Paper, we drew from existing statements of FIPPs as a starting point for principles that should apply in the commercial context, in particular the original principles developed by the Department of Health, Education and Welfare in 1973[7] and elaborations developed by the Organisation for Economic Co-operation and Development (OECD).[8] As we are developing in the Administration's forthcoming privacy White Paper, we seek to adapt these principles to the interactive and interconnected world of today. We are considering how best to incorporate principles that enable greater individual control over personal data and respect for the context in which such data was collected and that bring commercial data practices into alignment with reasonable consumer expectations. Notice and choice are fundamental to privacy protection, but today a more dynamic and holistic approach to privacy protection is needed, and obligations must be enforceable against the organizations that collect, use, and disclose personal data.

The Administration looks forward to working with Congress and stakeholders to define these protections and enforcement authorities further and enact them into law.

B. Implementing Enforceable Codes of Conduct Developed Through Multi-Stakeholder Processes

The Administration called for a dual approach to privacy protection, coupling legislative protection enshrined in a consumer privacy bill of rights with the adoption

---

[5] All comments that the Department received in response to the Green Paper are available at *http://www.ntia.doc.gov/comments/101214614–0614–01/*.

[6] For industry comments in support of legislation, see, *e.g.,* Intel Comment at 3 ("We disagree with the arguments some have advocated against the adoption of legislation, particularly that privacy legislation would stifle innovation and would hinder the growth of new technologies by small businesses. Instead, we believe that well-crafted legislation can actually enable small business e-commerce growth."); Google Comment at 2 (supporting "the development of a comprehensive privacy framework for commercial actors . . . that create[s] a baseline for privacy regulation that is flexible, scalable, and proportional"). For consumer groups and civil liberties' organizations comments in support of legislation, see, *e.g.,* Center for Democracy and Technology, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 2 ("CDT has long argued and continues to believe that the only way to implement a commercial data privacy framework that fully and effectively incorporates all the Fair Information Practice Principles is through baseline privacy legislation."); Center for Digital Democracy and USPIRG, Comment on Department of Commerce Privacy Green Paper, at 21 ("[W]e urge the adoption of regulations that will ensure that consumer privacy online is protected. The foundation for such protection should be the implementation of Fair Information Practices for the digital marketing environment."); Consumers Union, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 2 ("Consumers Union supports the adoption of a privacy framework that will protect consumer data both online and offline. . . . CU believes this comprehensive privacy framework should be grounded in statute. . . ."); Privacy Rights Clearinghouse, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 2 ("[N]oting that consumer trust is pivotal to commercial success online, and that it has diminished with industry self-regulatory practices, PRC advocates comprehensive federal FIPPs-based data privacy legislation.").

[7] *See* U.S. Dept. of Health, Education and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, July 1973, *http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm*.

[8] *See* OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, *http://www.oecd.org/document/18/0,3343,en__2649__34255__1815186__1__1__1__1,00.html*.

of legally enforceable codes of conduct developed through a multi-stakeholder process. The process should permit everyone who has a stake in privacy—companies, consumers, civil liberties advocates, academics, and others—to work together to take the statutory baseline privacy protections and expand them into legally enforceable best practices or codes of conduct. In such a process, the government is an active participant, a convener that brings together all participants and facilitates discussions, but does not prescribe the outcome. This process should be open to any person or organization that is willing to participate in the hard work of engaging with other stakeholders to resolve any substantive differences fairly and openly.

The Administration believes that the flexibility provided by multi-stakeholder processes could offer the most effective solution to the challenges posed by a rapidly changing technological, economic, and social environment. This recommendation reflects the Department's view that government must support policy development processes that are nimble enough to respond quickly to consumer data privacy issues as they emerge and that incorporate the perspectives of all stakeholders to the greatest extent possible. A well-crafted multi-stakeholder process will allow stakeholders to address privacy issues in new technologies and business practices without the need for additional legislation, permit stakeholders to readily reexamine changing consumer expectations, and enable stakeholders to identify privacy risks early in the development of new products and services.

Multi-stakeholder processes can be well suited for illuminating the policy tradeoffs inherent in such ideas like data breach notification, data security compliance, and Do-Not-Track. Starting with the commercialization of the Internet, the FTC has used a variety of stakeholder engagements to develop consumer data privacy policies. Its current work on Do-Not-Track carries on this history, and I applaud the leadership of Chairman Leibowitz,[9] as well as browser developers, Internet companies, standards organizations, privacy advocates, and others to provide options for greater control over personal information that may be used for online tracking.[10] The development of safe harbor programs is another task that can be addressed through the multi-stakeholder process recommended in the Commerce Green Paper.

C. Strengthening the FTC's Authority

Bolstering the FTC's enforcement authority is a key element of the Administration's proposed framework. In addition to its leadership in developing consumer data privacy policy, the FTC plays a vital role as the nation's independent consumer privacy enforcement authority for non-regulated sectors. Granting the FTC explicit authority to enforce baseline privacy principles would strengthen its role in consumer data privacy policy and enforcement, resulting in better protection for consumers and evolving standards that can adapt to a rapidly evolving online marketplace.

D. Establishing Limiting Principles on Consumer Data Privacy Legislation

As the Committee considers consumer data privacy legislation, I would like to reiterate the Administration's views on the limitations that Congress should observe in crafting legislation that strengthens consumer privacy protections and encourages continuing innovation. Legislation should not add duplicative or overly burdensome regulatory requirements to businesses that are already adhering to the principles in baseline consumer data privacy legislation. Legislation should be technology-neutral, so that firms have the flexibility to decide how to comply with its requirements and to adopt business models that are consistent with baseline principles but use personal data in ways that we have not yet contemplated. Furthermore, domestic privacy legislation should provide a basis for greater transnational cooperation on consumer privacy enforcement issues, as well as more streamlined cross-border data flows and reduced compliance burdens for U.S. businesses facing numerous foreign privacy laws.

IV. The Department of Commerce's Next Steps on Internet Privacy Policy

As discussion of consumer privacy legislation moves forward, the Department of Commerce will continue to make consumer data privacy on the Internet a top priority. We will convene Internet stakeholders to discuss how best to encourage the development of enforceable codes of conduct, in order to provide greater certainty for businesses and necessary protections for consumers. The past 15 years have shown that self-regulation without government leadership can be sporadic and in-

[9] *See* Statement of the Federal Trade Commission, before the Committee on Commerce, Science, and Transportation, U.S. Senate, Mar. 16, 2011, *http://www.ftc.gov/os/testimony/110316consumerprivacysenate.pdf*.

[10] *See, e.g.,* W3C Workshop on Web Tracking and User Privacy, Apr. 28–29, *http://www.w3.org/2011/track-privacy/* (collecting position papers and reporting on a workshop discussion of technical and policy approaches to limit web tracking).

sufficiently motivated. The Department received significant stakeholder support for the recommendation that it play a central role in convening stakeholders. A broad array of organizations, including consumer groups, companies, and industry groups, announced their support for the Department to help coordinate outreach to stakeholders to work together on enforceable codes of conduct.[11] This will be led by the National Telecommunications and Information Administration (NTIA) but would involve all relevant Commerce components, just as NTIA supports NIST's effort to convene stakeholders to discuss privacy issues that may arise in the implementation of the National Strategy for Trusted Identities in Cyberspace (NSTIC),[12] and ITA administers efforts relating to the U.S.-EU Safe Harbor Agreement[13] and the Asia-Pacific Economic Cooperation's (APEC) Cross-Border Data Privacy Rules. Through the National Science and Technology Council subcommittee I co-chair with Assistant Attorney General Christopher Schroeder, it will involve other Federal Government components, including the FTC.

The Department will also continue to work with others in the Federal Government to develop the Administration policy on data security. Without data security, there can be no effective data privacy. Last month, the Administration submitted a legislative proposal to improve cybersecurity, which includes a national data breach reporting provision.[14] Such a law would help businesses by simplifying and standardizing the existing patchwork of 47 state laws with a single, clear, nationwide requirement, and would help ensure that consumers receive notification, when appropriate standards are met, no matter where they live or where the business operates.

Earlier this month, the Department of Commerce released a green paper on Cybersecurity, Innovation, and the Internet Economy directed at increasing security beyond core critical infrastructure in the vital Internet and information technology sectors.[15] We are currently soliciting comments from stakeholders to help us develop this critical strategy, with the goal of improving security at home and around the world so that Internet services can continue to provide a vital connection for trade and commerce, as well as for civic participation and social interaction.

The Department will also support the Administration's efforts to encourage global interoperability by stepping up our engagement in international policymaking bodies. U.S. enterprises continue to incur substantial costs complying with disparate data privacy laws around the world. The need to comply with different privacy laws can lead to compartmentalization of data and privacy practices, can require a significant expenditure of time and resources, and can even prevent market access. Consistent with the National Export Initiative goal of decreasing regulatory barriers to trade and commerce, the Department will work with our allies and trading partners to facilitate cross-border data flows by increasing the global interoperability of privacy frameworks. Privacy laws across the globe are frequently based on similar values and a shared goal of protecting privacy while facilitating global trade and growth. The Department will work with our allies to find practical means of bridging any differences, which are often more a matter of form than substance. Specifically, the Department will work with other agencies to ensure that global privacy interoperability builds on accountability, mutual recognition and reciprocity, and enforcement cooperation principles pioneered in the OECD and APEC. The continued development of agreements with other privacy authorities around the world, coordinated with the State Department and other key actors in the Federal Government, could further reduce significant business global compliance costs.

Congressional action in this area at this time can have a significant global impact. The Administration's work on consumer data privacy is having a significant and positive effect on our discussions with members of the European Union. One illus-

---

[11] *See, e.g.,* Center for Democracy and Technology, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 15; Consumers Union, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 2–3; Microsoft, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 6; Walmart, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 2; Intel, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 7; Google, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 5; Facebook, Comment to Department Privacy Green Paper, Jan. 28, 2011, on 13; and Yahoo!, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 11.

[12] National Strategy for Trusted Identities in Cyberspace (NSTIC), Apr. 15, 2011, *http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.*

[13] *See Export.gov,* Welcome to the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks (last updated Mar. 31, 2011), *http://www.export.gov/safeharbor/.*

[14] *See* Statement for the Record of Philip Reitinger, Deputy Under Secretary, National Protection and Programs Directorate, before the Senate Homeland Security and Governmental Affairs Committee: "Protecting Cyberspace: Assessing the White House Proposal," May 23, 2011.

[15] Cybersecurity, Innovation and the Internet Economy, June 11, 2011, *http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf.*

tration of this direction comes from a May 18, 2011, speech about the reform of the EU Data Protection Directive by European Justice Commissioner Viviane Reding. Commissioner Reding stated that "EU-U.S. cooperation on data protection is crucial to protect consumers and enhance legal security for businesses online. I welcome a draft Bill of Rights just introduced in the U.S. Congress as a bipartisan initiative of Democrats and Republicans." Commissioner Reding also stated that "[t]his is a good opportunity to strengthen our transatlantic cooperation." Last week I was in Budapest to speak with European data privacy commissioners and, while we have much further to go in our discussions with Europe, and much remains uncertain about the final shape of the EU's revised Data Privacy Directive, we see encouraging signs of potential for interoperability and harmonization from the other side of the Atlantic. U.S. enactment of legislation establishing comprehensive commercial data privacy protections will help. Strong leadership in this area could form a model for our partners currently examining this issue, and prevent fragmentation of the world's privacy laws and its concomitant increase in compliance costs to our businesses that conduct international trade.

V. Conclusion

Mr. Chairman, thank you again for the opportunity to provide our views on legislation to protect consumer privacy and promote innovation in the 21st Century. We look forward to working with you, the FTC and other federal agencies, the Executive Office of the President, and other stakeholders toward enactment of these consumer data privacy protections. I welcome any questions you have for me. Thank you.

The CHAIRMAN. Your statement will be included in the record.
Mr. KERRY. Thank you.
The CHAIRMAN. And thank you for your testimony.
Mr. Schlick.

STATEMENT OF AUSTIN C. SCHLICK, GENERAL COUNSEL, FEDERAL COMMUNICATIONS COMMISSION

Mr. SCHLICK. Good morning, Chairman Rockefeller, members of the Committee. Thank you for this opportunity to discuss the programs of the Federal Communications Commission to protect consumer privacy and data security. I am particularly pleased to be here this morning with two strong partners in that effort, the Department of Commerce and the Federal Trade Commission.

The FCC has decades of experience implementing privacy protection statutes. These include provisions of the Communications Act that required communications providers to safeguard their customers' personally identifiable information, as well as provisions to protect consumers against unwanted telephone and fax solicitations.

At the same time, increased use of personal data in connection with new online and wireless applications is raising serious privacy and security concerns. As the FCC recognized in the National Broadband Plan, successfully addressing these concerns will be critical to increasing adoption and deployment of technologies that benefit consumers, government, and the economy.

The Commission historically has focused on three privacy related goals: ensuring that personal information is protected from misuse and mishandling, requiring providers to be transparent about their practices, and enabling consumers to make informed decisions. These goals remain our primary focus as we implement the various sections of the Communications Act that directly impact privacy.

For example, Section 222 of the Communications Act requires telecommunications carriers and interconnected Voice-over-Internet Protocol providers to secure customer proprietary network informa-

tion, which is known as CPNI. CPNI includes consumers' call records and call information.

Under Section 222, the FCC has adopted rules addressing the handling, use, and sharing of CPNI. We have also adopted rules to prevent pretexting, a practice under which unauthorized third parties attempt to gain access to telephone subscribers' personal information.

Through our rulemakings and enforcement, we have resolved difficult issues such as when opt-in and opt-out notifications are appropriate, minimum notice standards, data sharing rules, reasonable data security measures, and notification to law enforcement and consumers in the event of data breaches. In just the last 6 months, the Commission issued 28 warnings and notices of apparent liability for various CPNI violations. Because of our active enforcement and education efforts, the Section 222 protections are now well-known and well understood, and the number of consumer complaints the FCC receives on CPNI issues has declined steadily.

Sections 338 and 631 of the Communications Act also protect personal information. These provisions establish requirements for satellite and cable television providers' treatment of their subscribers' personally identifiable information. The requirements include clear and conspicuous notice about collection and use of subscribers' personal data, limiting disclosure of personal data, and remedies for subscribers who suffer a violation of these provisions.

Working in parallel with the FTC, the FCC adopted do-not-call regulations under Section 227 of the Communications Act. Since 2009, we have issued nearly 150 warnings, citations, and other actions for do-not-call violations. The FCC and the FTC also collaborate on implementation of the CAN–SPAM Act, with the FCC adopting rules that prohibit sending unwanted commercial e-mail messages to wireless accounts without prior permission. The FCC and the Department of Justice enforce Section 705 of the Communications Act which prohibits unauthorized interception of radio communications and unauthorized disclosure of wire or radio communications.

The FCC supports consumer education in the areas of privacy and information security. The FCC is a partner in OnGuard-Online, an online initiative led by the FTC that helps consumers guard against Internet fraud and identity theft, protect their children's personal information, and avoid e-mail and phishing scams. The FCC also is a member of the National Initiative for Cybersecurity Education partnership led by the Department of Commerce.

Just yesterday, we held a workshop of the Commission on location-based wireless services and privacy issues that they raise. At this webcast event in which the FTC participated, we gathered information from wireless carriers, application developers, and business and academic leaders about trends in the development and use of location-based services, industry best practices for protecting personal information, and what consumers and parents should know about protecting themselves when using these services. We heard about the many potential benefits of location-based technologies, as well as the challenges of educating consumers to protect their privacy while using these new products and services.

The FCC brings to these issues accumulated privacy expertise, as well as expertise about new communications technologies and services. Protecting privacy is a necessary part of providing communications services. So, too, it is part of the FCC's mandate to promote a healthy and competitive communications marketplace that meets consumers' needs.

Thank you for this opportunity to testify today, and I look forward to your questions.

[The prepared statement of Mr. Schlick follows:]

PREPARED STATEMENT OF AUSTIN C. SCHLICK, GENERAL COUNSEL, FEDERAL COMMUNICATIONS COMMISSION

Good morning Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee. Thank you for this opportunity to discuss the Federal Communications Commission's programs to protect consumer privacy. I am particularly pleased to be here with representatives of two strong partners in this effort, the Department of Commerce and the Federal Trade Commission.

The FCC has decades of experience implementing privacy protection statutes. These include provisions of the Communications Act that require communications providers to safeguard their customers' personally identifiable information, as well as provisions that protect consumers against unwanted telephone and fax solicitations.

At the same time, increased use of personal data in connection with new online and wireless applications is raising serious privacy and security concerns. As the FCC recognized in the National Broadband Plan, successfully addressing these concerns will be critical to increasing adoption and deployment of technologies that benefit consumers, government, and the economy.

The Commission historically has focused on three privacy-related goals: ensuring that personal information is protected from misuse and mishandling; requiring providers to be transparent about their practices; and enabling consumers to make informed decisions. These goals remain our primary focus as we implement the various sections of the Communications Act that directly impact privacy.

For example, Section 222 of the Communications Act requires telecommunications carriers and interconnected Voice over Internet Protocol providers to secure customer proprietary network information, which is known as CPNI. CPNI includes consumers' call records and call-location information.

Under Section 222, the FCC has adopted rules addressing the handling, use, and sharing of CPNI. We also have adopted rules to prevent pretexting, a practice by which unauthorized third parties attempt to gain access to telephone subscribers' personal information. Through our rulemakings and enforcement, we have resolved difficult issues such as when opt-in and opt-out notifications are appropriate, minimum notice standards, data sharing rules, reasonable data security measures, and notification to law enforcement and consumers in the event of data breaches.

In just the last 6 months, the Commission issued 28 warnings and Notices of Apparent Liability for various CPNI violations. Because of our active enforcement and education efforts, the Section 222 protections are now well-known and well-understood, and the number of consumer complaints the FCC receives on CPNI issues has declined steadily.

Sections 338 and 631 of the Communications Act also protect personal information. These provisions establish requirements for satellite and cable television providers' treatment of their subscribers' personally identifiable information. The requirements include clear and conspicuous notice about collection and use of subscribers' personal data, limiting disclosure of personal data, and remedies for subscribers who suffer a violation of these provisions.

Working in parallel with the FTC, the FCC adopted "Do-Not-Call" regulations under Section 227 of the Communications Act. Since 2009, we have issued nearly 150 warning citations for Do-Not-Call violations. The FCC and the FTC also collaborate on implementation of the CAN–SPAM Act, with the FCC adopting rules that prohibit sending unwanted commercial e-mail messages to wireless accounts without prior permission.

The FCC and the Department of Justice enforce Section 705 of the Communications Act, which prohibits unauthorized interception of radio communications and unauthorized disclosures of wire or radio communications.

The FCC supports consumer education in the areas of privacy and information security. The FCC is a partner in On Guard Online, an online initiative led by the FTC that helps consumers guard against Internet fraud and identity theft, protect their children's personal information, and avoid e-mail and phishing scams. The FCC also is a member of the National Initiative for Cybersecurity Education partnership led by the Department of Commerce.

Just yesterday, we held a workshop at the Commission on location-based wireless services and the privacy issues they raise. At this webcast event in which the FTC participated, we gathered information from wireless carriers, application developers, and business and academic leaders about trends in the development and use of location-based services, industry best practices for protecting personal information, and what consumers and parents should know about protecting themselves while using these services. We heard about the many potential benefits of location-based technologies, as well as the challenges of educating consumers to protect their privacy while using these new products and services.

The FCC brings to these issues accumulated privacy expertise, as well as expertise about new communications technologies and services. Protecting privacy is a necessary part of providing communications services. So too, it is part of the FCC's mandate to promote a healthy and competitive communications marketplace that meets consumers' needs.

Thank you for the opportunity to testify today, and I look forward to your questions.

The CHAIRMAN. Thank you, Mr. Schlick.

We're going to proceed to the questions. And as for myself, they'll be rather rapid, because we do have votes at 11 o'clock, and that's very disconcerting to me. The Majority Leader failed to check with me about the convenience of the Commerce Committee. So I'll do the best I can. I'm going to ask these fairly quickly.

Commissioner Brill, as you know, Senator Pryor and I have introduced S. 1207, the Data Security and Breach Notification Act. What are your thoughts on this bill, quickly?

Ms. BRILL. The Commission supports strong federal legislation dealing with data security and breach notification, just like this bill. And this bill does satisfy the requirements of such a strong protective bill.

The CHAIRMAN. Thank you. Our bill gives the Federal Trade Commission rulemaking authority to require companies with large databases to adopt security protocols to protect consumer data. Do you think companies are doing enough to maximize protection of their databases?

Ms. BRILL. Companies can do more. We have brought many data security cases over the past several years. We've investigated many more. We are not seeing cases that are close calls. These are cases where companies are falling down on basic security measures, sometimes not even following their own security procedures. So, yes, companies can definitely do more in the area of data security.

The CHAIRMAN. I thank you. To follow up, the Commission has taken numerous enforcement actions against companies like Twitter for not adequately securing consumer information. Can you talk about how Senator Pryor's and my bill will complement your existing enforcement efforts?

Ms. BRILL. It actually will complement our efforts very well. Not only does it set forth some basic security processes and procedures, like having an officer focused on privacy, having within companies a process to deal with—excuse me—an officer focused on security and having in place processes to deal with security, but it also gives us broad rulemaking authority which will be very helpful. And, most importantly, I think, from my perspective, it gives us

civil penalty authority which, I think, will incentivize companies to improve their security practices before they ever have to deal with us.

The CHAIRMAN. Thank you. Incidentally, you're going to keep your building. Don't worry about it.

Ms. BRILL. Thank you.

The CHAIRMAN. Mr. Kerry, the Department of Commerce has also cause for a national data security legislation. Do you have any opinions on the bill that Senator Pryor and I have introduced?

Mr. KERRY. Senator Rockefeller, the bill certainly responds to the need for national legislation. One of the important drivers in the area of privacy has been the adoption of breach notification laws by states. There are now some 47 states that have them.

But in order to make those consistent and to drive the issue nationally, there is a need for national data breach notification laws. It is part of the Administration's cyber security package. And I thank you, Senator, for your leadership in helping to drive that issue.

The CHAIRMAN. Thank you, sir.

Commissioner Brill?

Ms. BRILL. Yes.

The CHAIRMAN. How does the FTC work with the Department of Justice on data security issues under current law?

Ms. BRILL. Generally speaking——

The CHAIRMAN. I haven't finished.

Ms. BRILL. Excuse me.

The CHAIRMAN. But my questioning is of clear purpose. Do you have a good working relationship that adequately furthers the public interest of protecting consumers and prosecuting criminals, or do we need to grant Justice more authority than it already possesses?

Ms. BRILL. It is important for the Department of Justice to have all the tools that it needs to go after folks who are hacking into databases. And to the extent that they feel that they need more tools, we, obviously, would support that.

But at the same time, it's critically important to recognize that we're never going to be able to catch all the criminals. We're never going to be able to catch all the hackers.

So what's critically important and what your bill, I think, does very well is it ensures that companies are going to shore up their data protection practices in the first instance so they aren't affected by hacks to the extent that we can prevent that. And that's why we appreciate your bill and what it does, especially in incentivizing companies to have good, strong programs in place, for instance, through the civil penalty provision.

The CHAIRMAN. Thank you. I've got 40 seconds left. Commissioner Brill, many companies are already offering consumers the ability to use web browsers that have a do-not-track mechanism on them. However, when consumers use this feature, no one is honoring this request except for one company, which would happen to be the Associated Press.

As of now, do you think the FTC can take action against consumers that do not honor a consumer's do-not-track request?

Ms. BRILL. Action against companies that don't honor it? If a company promises to honor a consumer's request, or an ad network promises to honor a consumer's request, then we can proceed fairly easily if they breach that promise through our deception enforcement jurisdiction.

But if a company does not make a promise to adhere to a consumer's request, then our jurisdictional test is a little bit more difficult to meet. We fall under our unfairness jurisdiction, and there are some challenges in meeting that kind of a test in a scenario like you've described. It would depend on the facts and circumstances.

The CHAIRMAN. I thank you.

Senator Kerry?

Senator KERRY. Thank you, Senator Rockefeller. I was struck by the opening, frankly, comments of Senator Toomey, the Ranking Member of the Subcommittee. And I think it's important if—if some of those questions are being raised, it's really important that they be addressed here.

And I wasn't planning to, but I want to use the time, because we've got a problem here in trying to get a general consensus and pass legislation if there's not a baseline level of understanding or acceptance of what we're dealing with. Senator Toomey, in fairness, is at another hearing that he has to be at in the Banking Committee. But I want the record to at least reflect the answers to this, and I know his staff will help make sure that he sees them.

But, you know, he stated very clearly the question. He raised the question of whether or not this is a solution in search of a problem and, in addition, wondered sort of what the harm is out there.

I think it's really important for the three of you to address that very directly. What is the harm? Is there harm or isn't there harm? Is this worth a national response? Is it imperative to have a national response? And, if so, can one be constructed without the unintended consequences of harming commerce and the open architecture?

I've been on this committee for a long time now, and I have fought diligently to protect the open architecture, not to tax, have net neutrality, do all the things necessary. But I do believe that it's imperative to have some kind of standard by which people are acting here.

So I want to begin with you, Commissioner Brill, since your regulatory agency is particularly in the line of fire on this, and then go to the Communications and end with the Commerce Department, if we could. But what is the harm? Is there harm? Is it real? Why do we—what should be compelled? And is this, indeed, a solution looking, you know, for a problem?

Ms. BRILL. I don't believe the focus on privacy protection is a solution looking for a problem. I think right now, consumers are very unaware of what's happening with their information, as I tried to communicate in my opening statement.

Just with respect to privacy notices, for instance, as one example, and thinking about mobile technology, there have been studies that have shown that apps which a lot of young people are using—teenagers, young adults—many of them don't even have any kind of privacy policy whatsoever. To the extent that they do have a pri-

vacy policy, it often requires consumers to click through literally over a hundred screens in order to read the privacy policy.

This just isn't reasonable to expect consumers to be able to do that in this modern technological age. So we need to come up with some solutions that fit the new technology that give consumers information that they need about how their information is being used, and then giving them some choices about it.

Mr. SCHLICK. Senator Kerry, there absolutely is a problem. We've seen that in our own Section 222——

Senator KERRY. Also, is there harm?

Mr. SCHLICK. Yes.

Senator KERRY. Is there harm here?

Mr. SCHLICK.—in Section 222 implementation—to give you a concrete example, pretexting. The Electronic Privacy Information Center came to us a few years ago and identified the problem of data being insufficiently secure and being taken out through the pretexting practices on false pretenses and sold commercially to the harm of consumers. So this was one instance where we conducted a rulemaking and were able to adopt rules to limit and end that practice.

Our National Broadband Plan looks beyond the harmed individuals and to the harm of the economy. A key finding of the Broadband Plan was that if consumers and application developers don't understand and trust the rules for privacy protection that are built into the system, then the adoption by consumers, the deployment by network operators of broadband technologies will be harmed.

We saw this again in our location-based service forum yesterday, where consumer groups and industry agreed that there is a need for clear rules of the road so that there will be an ability and a willingness to use these services for the benefit of consumers as well as industry.

Mr. KERRY. Senator, let me say that our support for legislation comes from an extensive exchange with members of the public, with members of the business community, who broadly, across a spectrum of the business community, retail industries, as well as technology industries, as well as companies engaged in international trade, said to us that there was a need for government action and privacy protection. And it's unusual for a government agency to propose regulation and to have a wide spectrum of the business community as well as consumers and others endorse that proposal. But that's precisely what occurred when we put out the commerce green paper in December.

I think what that stems from is the critical need for trust in the sector. Let me tell you the story of a policy conference that I participated in a couple of years ago with a spectrum of people from business, from government, from academia, across the political spectrum, given the exercise to identify key risks and key drivers to the digital economy and to the development of broadband. And working in four separate groups looking at scenarios, every single one of them came up with the same risks, the same drivers. And every single one of them independently framed it in the same way as trust. And I think, if we look today at the wave of breaches that

Senator Rockefeller alluded to, you know, we are facing a higher risk scenario in which trust is eroding.

And, you know, there are a lot of companies that have good practices, that understand the importance of trust to their business models, their survival. There are malicious actors and outliers there who exploit that trust.

The CHAIRMAN. Thank you, Senator.

Senator Wicker.

STATEMENT OF HON. ROGER F. WICKER,
U.S. SENATOR FROM MISSISSIPPI

Senator WICKER. Mr. Chairman, I'm going to yield my time. I hope we're able to get to the second panel before the series of seven votes begins.

The CHAIRMAN. We won't, but we're coming back. OK. We have no choice.

Senator WICKER. I understand that, and I yield my time.

The CHAIRMAN. All right.

Then Senator Ayotte.

STATEMENT OF HON. KELLY AYOTTE,
U.S. SENATOR FROM NEW HAMPSHIRE

Senator AYOTTE. Thank you, Mr. Chairman.

Mr. Kerry, I understand that the Department of Commerce has led this Internet Policy Task Force. But could you also explain for us what the role of the Department of Commerce would be? Do you envision any enforcement role going forward? I mean, obviously, I'm pretty clear as to what the FTC and FCC's role is, but if you can help us with that——

Mr. KERRY. Senator Ayotte, no, we do not envision an enforcement role. The FTC is a critical policymaker and the nation's enforcement authority over a broad area other than specific sectoral regimes like communications, like health records. And we believe that that role should be strengthened.

The role of the Department of Commerce is as a convener, as a policy leader for the Executive Branch. It's important that the Executive Branch have a voice in the process, that we be part of the debate, as we are here today. But we have worked closely with the FTC in developing policy in this area. We would continue to do so.

Senator AYOTTE. Thank you.

Commissioner Brill, I wanted to follow up on—as I know you share a history at the Attorney General's office——

Ms. BRILL. Exactly.

Senator AYOTTE.—in Vermont, so welcome.

Ms. BRILL. Thank you.

Senator AYOTTE. And I wanted to ask about the enforcement piece of, for example, a proposal for do-not-track legislation. And, particularly, when we get on areas where we're focused on a particular kind of technology, given the changes that we can see happen in the technology field, (a), how would you anticipate that we would—the enforcement mechanism would work for something like a do-not-track registry, number one. And then, second, do you have any concerns that a do-not-track policy could take away some of the tools that consumers have?

There have been some studies that show that this could harm online advertising. So I wanted to get your thoughts on those two issues.

Ms. BRILL. Sure. So just to be clear, Senator Ayotte, it would not be a registry. What we're talking about is a technology-driven solution that would be generated through browser companies or ad networks themselves or advertisers themselves.

In terms of enforcement, what we—we do want to see a strong enforcement component, whether it becomes a mechanism—or a mechanism set up by industry itself, or whether it gets set up through legislation. The key component in an enforcement mechanism is that those who receive the messages from consumers about the choices that they are making will honor them. And once we are assured, either through a self-regulatory mechanism or through legislation, that the receipt of a header or a cookie or whatever the technology is—when an entity receives that message—that they promise they will honor it. Then we have an enforcement tool.

So that's a critical piece here. And that is certainly something that we're looking to see happen in the industry-driven efforts that are currently underway.

OK. Your other point about could it take away the benefits—you know, there has been discussion about whether or not an overwhelming number of consumers would participate and, therefore, it would drive away the free content that's currently available on the Web. My view is that, actually, what will happen is consumers will have much more trust in what's happening on the Internet if they understand that the choice is available to them to make granular choices about what will happen with their information, how it will be used, and how it will be collected.

I actually don't expect that we'll see a whole lot of consumers opting into the system, I mean, you know, choosing to participate. But what it will do is it will, I think, give—just engender a huge amount of trust, which I think will actually cause the industry to thrive even more. I think that's the critical component here that I haven't heard a lot of discussion about.

Senator AYOTTE. And just to be clear, just so I understand, in terms of issues—for example, a do-not-track issue—you envision that this could be something implemented by industry as opposed to us in Congress coming up—because one of the issues I see in terms of implementation is for us to come up with a solution that will work in application is a very difficult task. And, often, we aren't the best ones to come up with those solutions.

Ms. BRILL. It can be done by industry. And we have called—a majority of the Commissioners have called on industry to step up to the plate. I have been a particularly vocal proponent of industry proceeding in a self-regulatory manner.

I think it has been slow. We started to make these calls to do something with respect to online behavioral advertising several years ago. But since we started making a specific call for do-not-track, industry has moved, and there has been significant progress on the part of industry.

I am worried, though, that we might not be able to get all the way there because of the way the industry is structured. Advertisers and ad networks are rather disparate. There are lots of

them. And unless we get them to sort of uniformly agree that they're going to participate and honor consumers' requests, I'm just not sure that the self-regulatory mechanism can work. So I'm worried about the way that it's structured right now—the industry is structured—as to whether we can get all the way there.

Senator AYOTTE. Thank you very much.

The CHAIRMAN. Thank you very much.

Before I go to Senator Klobuchar, we have a major problem to work out here. There are five votes that are starting at 11:05. I'm trying to get them moved to 11:10, which means we could spend another 15 minutes here.

We have another panel. We have Senator Klobuchar. Senator Pryor has just walked in. Now, you can decide what you want to do.

My recommendation would be that, Senator Klobuchar, you ask your question, because you've been here a while. Senator Pryor, who is the Subcommittee Chairman is all over this, and he's extremely important. But somebody has to sacrifice. And I think what we need to do is let Senator Klobuchar ask her question quickly and make sure it's responded to quickly. Then we call up the other panelists. We let them give their testimony, and then we submit questions to them in writing, and then all scramble to get to the Senate floor to vote on heavens knows what. Is that acceptable?

It's not to you, and I understand. Is that acceptable?

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Yes, ready to go.

The CHAIRMAN. Go ahead.

Senator KLOBUCHAR. OK. Well, thank you very much, Mr. Chairman. This issue, of course, can create divides, but I think we all know that there's some line in the sand here. And, for me, you know, when you order books on a Kindle and then they come up with recommendations of books that are similar to what you ordered, that's just fine. It's actually helpful and not harmful.

But on the other hand, when you hear stories of companies that may be compiling what they call "sucker lists" about consumers that may be susceptible to different kinds of fraud, that's a problem. And so I appreciate you helping us work through this today.

One of the things I wanted to ask you about, Commissioner Brill, was the Children's Online Privacy Protection Act and the Unfair and Deceptive Conduct Clause. It's not clear what regulations prohibit the sharing of user information on mobile phones. For example, if there is an application geared toward adults that has no user agreement or stated privacy policy but shares location and other mobile information with a third-party advertiser without seeking consent from the user, are there any enforcement mechanisms that the FTC can use to prosecute the company for misusing the person's data?

Ms. BRILL. Are you focused specifically on children——

Senator KLOBUCHAR. Mobile.

Ms. BRILL.—or mobile?

Senator KLOBUCHAR. No, this is on the mobile.

Ms. BRILL. So, if a mobile phone right now does not—a mobile—an application does not have a privacy policy and is collecting geo-location information, that's your question? Is there something that we can do about it? We are, then, as I mentioned a few moments ago, in a world where we're no longer dealing potentially with deception, because they haven't said anything that they are then not following through on, and we're rather in the realm of unfairness.

And in that realm, it really does depend on the facts and circumstances. It depends on how they're using it. We might be able to make out an argument that the particular use or the way in which geo-location was used would be unfair. There also might be an argument that failing to have a disclosure to consumers about the way in which geo-location was used, if it harms the consumer, would also be unfair. But it's a tougher test.

Senator KLOBUCHAR. OK. And then back to the children's issues, under the Children's Online Privacy Protection Act, companies operating websites or online services intended for children under 13 are prohibited from collecting information. And I just wonder if there is a practical—and I believe that is a good provision—but is there any practical way for the FTC to distinguish between websites and online services intended for children that need to comply with this law versus applications for adults?

Mr. BRILL. Sure, yes. So the Children's Online Privacy Protection Act applies when you have a website that is either directed at kids or where the website knows that it is collecting information about kids. And by kids, it's kids under 13.

In order to determine whether a website is directed at children, we really look at the totality of the circumstances. So we'll look at things like—are there cartoons being used? We'll look at issues in the mobile space. Where is the application being sold, or how is it being sold? What part of the app store is it in? Is it in the part of the app store that's designed for kids, or is it in a different part of the app store?

So those are the kinds of factors that we'll look at to determine whether the website or the mobile application is focused on children. In terms of whether or not the general audience website or application is collecting information about children, you know, if the website actually receives information from a teacher or a parent that there's a particular kid involved, obviously, then, they know.

But we also do undercover work, you know. We'll go online and pretend we're 13 or 12 or 11 and see if the website will collect information about us. So there are a number of different ways we can figure out what's happening.

Senator KLOBUCHAR. OK. One last question to Mr. Kerry.

I've been working on this Cloud Computing bill, as you know. And one of the issues here is that we are trading partners internationally, and I think we've talked about this before in Judiciary—but the need to establish privacy, security, and cross-border data flow standards along with working with our allies, do you believe it would be prudent to establish a global standard that companies in all countries would voluntarily subscribe to?

Mr. KERRY. That's a direction that we need to——

The CHAIRMAN. If you could answer in 30 seconds——

Mr. KERRY.—move toward, Senator Klobuchar. I mean, one of the key tenets of what we're trying to do is to establish global interoperability so that companies can trade, so that data can reside transparently in different locations in the cloud. So to try to bring global privacy standards closer together is an important part of our support of comprehensive legislation.

The CHAIRMAN. Thank you. We're now on this rather quickened pace. I thank all three of you very much.

And I want to introduce—Senator Begich, I'll explain this to you on the way to a vote, how you've been abused.

The second panel are Mr. Scott Taylor, Vice President, Chief Privacy Officer, Hewlett-Packard; Mr. Stuart Pratt, President and CEO, Consumer Data Industry Association; Ms. Ioana Rusu, Regulatory Counsel, Consumers Union; Mr. Tim Schaaff, President, Sony Network Entertainment International; and Mr. Thomas Lenard, President and Senior Fellow, Technology Policy Institute.

And, once again, our purpose here will be in the time remaining to us—which is not yet determined, but let's say it's 20 minutes at the maximum—for all 5 of you to give testimony. That is a challenge, but you're exceptionally bright, well-educated, and advanced people, and so you should be able to meet it.

And we will start with you, Mr. Pratt.

And, incidentally, the questions will be submitted from the Committee members to all of you.

STATEMENT OF STUART K. PRATT, PRESIDENT AND CEO, CONSUMER DATA INDUSTRY ASSOCIATION

Mr. PRATT. Chairman Rockefeller, members of the Committee, thank you for this opportunity to appear before you today. And for the record, my name is Stuart Pratt, and I'm the CEO of the Consumer Data Industry Association.

The CHAIRMAN. We know that. Get right to the point.

Mr. PRATT. CDIA's members' data and technologies protect consumers and help businesses manage risk. Whether it's counterterrorism efforts, locating a child who has been kidnapped, preventing a violent criminal from taking a job with access to children or the elderly, or ensuring the safety and soundness of lending decisions, our members' databases, software, and analytical tools are critical to how we manage risk in this country, ensure consumers are treated fairly, and how we protect consumers from becoming victims for both violent and white-collar crimes.

Let me just skip some of the examples. Those are in the record. And let's jump to some of the key points. I think that's where you're driving us here.

I think this committee has some—a tremendous opportunity before it here today. First of all, it can fill an important gap in current law by ensuring that all U.S. businesses which are not already subject to data security for sensitive personal information are in the future. CDIA is on record in support of enacting national standards for securing personal information, and we're pleased to have this opportunity to affirm this position again today.

Second, Congress can complete the good work of 48 states which have enacted data breach notification laws by creating a much-needed national standard which ensures consumers are treated in

the same way, no matter where they live. Here again, the CDIA is happy to support the enactment of such a standard for those who possess sensitive personal information and where such information has been stolen or lost, the consumer is exposed to a significant risk of becoming a victim of identity theft.

New law regarding data security and data breach notification should be designed to align with current laws which are already robust and effective. CDIA's members are financial institutions under the Gramm-Leach-Bliley Act and as such, they are already subject to an appropriate standard for securing sensitive personal information. It is important that new law not interfere with, alter, or add to the requirements of the GLB safeguards rule and the enforcement guidance that has evolved over a decade of enforcement actions, examinations, and regulatory guidance.

The same principle applies to other sectors of the U.S. economy that have already been subject to their data security duties. This new law should fill gaps, thus ensuring that all sensitive personal information is protected.

Similarly, where sectors of the U.S. economy are already subject to a federal data breach notification standard through law, regulation, or rules, these sectors should be exempted from having to comply with the duties of a new federal standard. Again, the new federal standard should fill a gap.

In the past, bills have tried to eliminate the problems of imposing duplicative duties. However, these exemptions often fall short by using an in-compliance-with construction rather than a subject-to construction. Getting these exemptions right is important as the new duties for data security and data breach notification are enacted, and we urge the Committee to avoid creating duplicative law.

Congress must also avoid creating a 51st state law. Enacting strong and effective duties for securing sensitive personal information and data breach notification is only a success if it creates a true national standard for U.S. businesses. This is especially true for small businesses.

Finally, we would urge the Committee to exclude privacy issues which are not relevant to data security or data breach notification. Privacy and data security are not coterminous concepts. CDIA's members live with a variety of laws that regulate their businesses today, including the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, Title V, HIPPA, the Driver's Privacy Protection Act, and more. We urge this committee and the Congress to not comingle privacy concepts such as provisions which propose to regulate entities defined as information brokers with the duty to secure sensitive personal information and to provide notices to consumers where there has been a breach of their data.

As discussed more completely in my written testimony, privacy issues can even interfere with the development of data which is used to prevent fraud, identity theft, and to manage risks like those we have discussed. Let's move on clean data security and data breach notification which will inure benefits to consumers by establishing a national standard and ensuring that U.S. businesses can comply, which is always their highest goal.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Pratt follows:]

PREPARED STATEMENT OF STUART K. PRATT, PRESIDENT AND CEO, CONSUMER DATA INDUSTRY ASSOCIATION

Chairman Rockefeller, Ranking member Hutchison and members of the Committee, thank you for this opportunity to appear before you today. For the record, my name is Stuart K. Pratt and I am President and CEO of the Consumer Data Industry Association. My testimony will focus on:

- The importance to consumers of the data systems and analytical tools our members produce.
- How current laws which regulate our members' products already protect consumers.
- Separating privacy issues from the important work of establishing a national standard for securing sensitive personal information and data breach notification.
- Aligning new law with existing laws.
- Creating a truly national standard.

CDIA Members' Data and Technologies Protect Consumers and Help Us Businesses Manage Risk

Whether it is counterterrorism efforts, locating a child who has been kidnapped, preventing a violent criminal from taking a job with access to children or the elderly, or ensuring the safety and soundness of lending decisions our members' innovative databases, software and analytical tools are critical to how we manage risk in this country, ensure fair treatment and most importantly, how we protect consumers from becoming victims of both violent and white-collar crimes of all types.

Following are examples of how our members' products, software and databases bring material value to consumers and our country:

- Helping public and private sector investigators to prevent money laundering and terrorist financing.
- Ensuring lenders have best-in-class credit reports, credit scoring technologies, income verification tools and data on assets for purposes of making safe and sound underwriting decisions so that consumers are treated fairly and products make sense for them.
- Bringing transparency to the underlying value of collateralized debt obligations and in doing so ensuring our nation's money supply is adequate which militates against the possibility and severity of economic crises.
- Enforcing child support orders through the use of sophisticated location tools so children of single parents have the resources they need.
- Assisting law enforcement and private agencies which locate missing and exploited children through location tools.
- Researching fugitives, assets held by individuals of interest through the use of investigative tools which allow law enforcement agencies tie together disparate data on given individuals and thus to most effectively target limited manpower resources.
- Witness location through use of location tools for all types of court proceedings.
- Reducing government expense through entitlement fraud prevention, eligibility determinations, and identity verification.
- Making available both local and nationwide background screening tools to ensure, for example, that pedophiles don't gain access to daycare centers or those convicted of driving while under the influence do not drive school buses or vans for elder care centers.
- Helping a local charity hospital to find individuals who have chosen to avoid paying bills when they have the ability to do so.
- Producing sophisticated background screening tools for security clearances, including those with national security implications.
- Improving disaster assistance responses through the use of cross-matched databases that help first-responders to quickly aid those in need and prevent fraudsters from gaming these efforts for personal gain.

Not only do our members' technologies and innovation protect us and ensure that we are managing risk in this country, but they reduce costs and labor intensity.

Risk management is not merely the domain of the largest government agencies or corporations it is available to companies of all sizes thanks to our members' investments. Consider the following scenarios:

Scenario 1—Effective Use of Limited Resources

The following example was given during a Department of Homeland Security meeting on use of data by the department: "One extremely well-known law enforcement intelligence example from immediately post-9/11 was when there was a now well-publicized threat . . . that there might be cells of terrorists training for scuba diving underwater bombing, similar to those that trained for 9/11 to fly but not land—planes. How does the government best acquire that? The FBI applied the standard shoe-leather approach—spent millions of dollars sending out every agent in every office in the country to identify certified scuba training schools. The alternative could and should have been for the Federal Government to be able to buy that data for a couple of hundred dollars from a commercial provider, and to use that baseline and law enforcement resources, starting with the commercial baseline."

Scenario 2—Lowering Costs/Expanding Access to Best-in-Class Tools

One commercial database provider charges just $25 for an instant comprehensive search of multiple criminal record sources, including fugitive files, state and county criminal record repositories, proprietary criminal record information, and prison, parole and release files, representing more than 100 million criminal records across the United States. In contrast, an in-person, local search of one local courthouse for felony and misdemeanor records takes 3 business days and costs $16 plus courthouse fees. An in-person search of every county courthouse would cost $48,544 (3,034 county governments times $16). Similarly, a state sexual offender search costs just $9 and includes states that do not provide online registries of sexual offenders. An in-person search of sexual offender records in all 50 states would cost $800.

Scenario 3—Preventing Identity Theft & Limiting Indebtedness

A national credit card issuer reports that they approve more than 19 million applications for credit every year. In fact they process more than 90,000 applications every day, with an approval rate of approximately sixty percent. This creditor reports that they identify one fraudulent account for every 1,613 applications approved. This means that the tools our members provided were preventing fraud in more than 99.9 percent of the transactions processed. These data also tell us that the lender is doing an effective job of approving consumers who truly qualify for credit and denying consumers who are overextended and should not increase their debt burdens.

Current Laws Regulating Our Members' Products Protect Consumers and Are Robust

The United States is on the forefront of establishing sector-specific and enforceable laws regulating uses of personal information of many types. The list of laws is extensive and includes but is not limited to the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), The Gramm-Leach-Bliley Act (Pub. L. 106–102, Title V), the Health Insurance Portability and Accountability Act (Pub. L. 104.191), and the Drivers Privacy Protection Act (18 U.S.C. 2721 et seq.).

Following are more probative descriptions of some of these laws, the rights of consumers and also the types of products that fall within the scope of the law.

Fair Credit Reporting Act

Key to understanding the role of the FCRA is the fact that it regulates any use of personal information (whether obtained from a public or private source) defined as a consumer report. A consumer report is defined as data which is gathered and shared with a third party for a determination of a consumer's eligibility for enumerated permissible purposes. This concept of an eligibility test is a key to understanding how FCRA regulates an extraordinarily broad range of personal information uses. The United States has a law which makes clear that any third-party-supplied data that is used to accept or deny, for example, my application for a government entitlement, employment, credit (*e.g.,* student loans), insurance, and any other transaction initiated by the consumer where there is a legitimate business need. Again, this law applies equally to governmental uses and not merely to the private sector and provides us as consumers with a full complement of rights to protect and empower us. Consider the following:

- The right of access—consumers may request at any time a disclosure of all information in their file at the time of the request. This right is enhanced by re-

quirements that the cost of such disclosure must be free under a variety of circumstances including once per year upon request, where there is suspected fraud, where a consumer is unemployed and seeking employment, when a consumer places a fraud alert on his or her file, or where a consumer is receiving public assistance and thus would not have the means to pay. Note that the right of access is absolute since the term file is defined in the FCRA and it includes the base information from which a consumer report is produced.

- The right of correction—a consumer may dispute any information in the file. The right of dispute is absolute and no fee may be charged.
- The right to know who has seen or reviewed information in the consumer's file—as part of the right of access, a consumer must see all "inquiries" made to the file and these inquiries include the trade name of the consumer and upon request, a disclosure of contact information, if available, for any inquirer to the consumer's file.
- The right to deny use of the file except for transactions initiated by the consumer—consumers have the right to opt out of non-initiated transactions, such as a mailed offer for a new credit card.
- The right to be notified when a consumer report has been used to take an adverse action. This right ensures that I can act on all of the other rights enumerated above.
- Beyond the rights discussed above, with every disclosure of a file, consumers receive a notice providing a complete listing all consumer rights.
- Finally, all such products are regulated for accuracy with a "reasonable procedures to ensure maximum possible accuracy" standard. Further all sources which provide data to consumer reporting agencies must also adhere to a standard of accuracy which, as a result of the FACT Act, now includes new rulemaking powers for federal agencies.

Gramm-Leach-Bliley Act

Not all consumer data products are used for eligibility determinations regulated by the FCRA. Congress has applied different standards of protection that are appropriate to the use and the sensitivity of the data. We refer to these tools as Reference, Verification and Information services or RVI services. RVI services are used not only to identify fraud, but also to locate and verify information for the public and private sectors. Fraud prevention systems, for example, aren't regulated under FCRA because no decision to approve or deny is made using these data. Annually businesses conduct an average more than 2.6 billion searches to check for fraudulent transactions. As the fraud problem has grown, industry has been forced to increase the complexity and sophistication of the fraud detection tools they use. While fraud detection tools may differ, there are four key models used.

- Fraud databases—check for possible suspicious elements of customer information. These databases include past identities and records that have been used in known frauds, suspect phone numbers or addresses, and records of inconsistent issue dates of SSNs and the given birth years.
- Identity verification products—crosscheck for consistency in identifying information supplied by the consumer by utilizing other sources of known data about the consumer. Identity thieves must change pieces of information in their victim's files to avoid alerting others of their presence. Inconsistencies in name, address, or SSN associated with a name raise suspicions of possible fraud.
- Quantitative fraud prediction models—calculate fraud scores that predict the likelihood an application or proposed transaction is fraudulent. The power of these models is their ability to assess the cumulative significance of small inconsistencies or problems that may appear insignificant in isolation.
- Identity element approaches—use the analysis of pooled applications and other data to detect anomalies in typical business activity to identify potential fraudulent activity. These tools generally use anonymous consumer information to create macro-models of applications or credit card usage that deviates from normal information or spending patterns, as well as a series of applications with a common work number or address but under different names, or even the identification and further attention to geographical areas where there are spikes in what may be fraudulent activity.

The largest users of fraud detection tools are financial businesses, accounting for approximately 78 percent of all users. However, there are many non-financial business uses for fraud detection tools. Users include:

- Governmental agencies—Fraud detection tools are used by the IRS to locate assets of tax evaders, state agencies to find individuals who owe child support, law enforcement to assist in investigations, and by various federal and state agencies for employment background checks.
- Private use—Journalists use fraud detection services to locate sources, attorneys to find witnesses, and individuals use them to do background checks on childcare providers.

CDIA's members are also the leading location services providers in the United States. These products are also not regulated under FCRA since no decision is based on the data used. These services, which help users locate individuals, are a key business-to-business tool that creates great value for consumers and business alike. Locator services depend on a variety of matching elements. Consider the following examples of location service uses of a year's time:

- There were 5.5 million location searches conducted by child support enforcement agencies to enforce court orders. For example, the Financial Institution Data Match program required by the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (PL 104–193) led to the location of 700,000 delinquent individuals being linked to accounts worth nearly $2.5 billion.
- There were 378 million location searches used to enforce contractual obligations to pay debts.
- Tens of millions of searches were conducted by pension funds (location of beneficiaries), lawyers (witness location), blood donors organizations (blood supply safety), as well as by organizations focused on missing and exploited children.

Clearly RVI services bring great benefit to consumers, governmental agencies and to businesses of all sizes. Laws such as the Gramm-Leach-Bliley Act and Fair Credit Reporting Act are robust, protective of consumer rights, but also drafted to ensure that products used to protect consumers, prevent fraud and to locate individuals are allowed to operate for the good of consumers and business.

A National Data Security and Data Breach Notification Standard Is A Separate Matter from Privacy

Let me start by stating unequivocally that CDIA's supports the creation of a national standard for both securing sensitive personal information and notification of consumers when there has been a breach of that data. Our position is in agreement with the Federal Trade Commission recommendation offered in multiple testimonies on the Hill and via their joint Task Force report issued along with the Department of Justice. This committee can play a leading role in ensuring that such a standard is set. This committee can also ensure that privacy issues are not confused with the core consumer protections found in a proposal that focuses on data security and breach notification.

Provisions found in some bills that create national standards for security and notification also impose accuracy, access and correction standards on a certain type of entity defined as an information broker. We believe that provisions such as these should be struck because they do not advance the cause of protecting data, and they interfere with how other current laws regulate the development of products which do protect consumers. Consider the following:

Products such as those designed for fraud prevention and location are produced under laws such as the Gramm-Leach-Bliley Act and Section 5 of the Federal Trade Commission Act. The definition of information broker often does not exclude financial institutions regulated under GLB. Therefore products developed under the data-use limitations found in GLB Title V, Section 502(e) are adversely affected by information broker provisions.

Neither a product developed for fraud prevention nor location should be subject to accuracy, access and correction standards since neither product is used to deny or approve an application, etc. If they were designed for the purpose of making decisions about a consumer's eligibility, then they would already be regulated under the FCRA. Further accuracy, access and correction standards are not relevant to the important work of this Committee to establish a national standard for securing sensitive personal information and notifying consumers when there is a breach of such data.

Consider the effect of applying an accuracy standard to fraud tools. Ironically doing so would lead to interference with the very tools that help protect consumers against the risks posed by failures to protect sensitive personal information. Fraud prevention tools are built based on data about consumers, data about confirmed fraud attempts, data about combinations of accurate and inaccurate data used for

fraud attempts and more. Fraud tools are designed to identify transactions or applications that are likely to be fraudulent in order to allow the user to take additional steps to prevent the crime and still process legitimate transactions.

Similarly it is wrong to subject fraud prevention tools to an access and correction regime. If details of a fraud tool are disclosed it is akin to disclosing the recipe for fraud prevention. This result works against a bill which is focused on protecting consumers from crime, particularly identity theft.

As discussed in this testimony, location and investigative research services are materially important to how risk is managed. They are not designed to be used for decisionmaking and thus are not regulated under the FCRA, which already regulates all data used for eligibility decisions (including the imposition of accuracy, access and correction rights). Such services are, for example, designed to help a user identify possible connections between disparate records and ultimately possible locations for the subject of the search. Measuring the quality of the possible connections is not akin to an accuracy standard, nor should an accuracy standard be applied to "possible matches." Further, providing access to a database for purposes of error correction could affect the quality of the systems since matches are sometimes based on combinations of accurate and inaccurate data.

Accuracy, access and correction duties are best left to future debates about privacy, but they have no relevance to data security and breach notification.

Aligning the Operation of New and Current Law

As discussed above, by not including privacy issues (information brokers/accuracy/access/correction) in a data security and notification bill, the committee avoids many problems with the operation of effective federal laws that are on the books today (*e.g.,* FCRA, GLB, HIPAA, DPPA, etc.). Further the committee's bill should not create overlapping burdens where U.S. companies are already in compliance with a security breach notification or security standard for sensitive personal information. For example, financial institutions which are subject to the data security standards of the Gramm-Leach-Bliley Act and also federal agency guidance regarding data breach notification should be fully exempted from the bill.

The Importance of a National Standard

Congress should not enact a fifty-first law. A true national standard will benefit consumers because they will enjoy the benefits of this standard no matter where they live. Such a standard also benefits U.S. businesses of all sizes because they can then be successful in the goal they all share and that is to protect consumers' sensitive personal information by building data security into their entire enterprise and to notify consumers where there is a significant risk of identity theft.

Conclusion

This committee has a number of important opportunities:

- To fill an important gap in current law by ensuring that all U.S. businesses which are not already subject to a data security duty for sensitive personal information are in the future.
- To harmonize the 48 state data breach notification duties and in doing so create much needed uniformity.
- To exclude privacy issues which are not relevant to data security and breach notification.
- To avoid creating law which interferes with the operation of current laws already on the books.
- To create an effective national standard for securing sensitive personal information and data breach notification.

We thank you again for giving us this opportunity to testify. It is only through such dialogue that good laws are enacted. I'm happy to answer any questions.

The CHAIRMAN. Thank you very much.
Ms. Rusu.

STATEMENT OF IOANA RUSU, REGULATORY COUNSEL, CONSUMERS UNION

Ms. RUSU. Thank you, Chairman and members of the Committee. I'm going to skip over the intro and jump right into it.

I think we can all agree that technological advances over the past decade have created incredible, fantastic tools for consumers to use. However, privacy is still important and relevant today. Even in today's age of extensive sharing, few people would agree that every piece of information about them should be available to everyone for any conceivable purpose.

In fact, in a May 2011 Consumer Reports poll, 82 percent of respondents were concerned that companies may be passing on their personal information to third parties without their permission. Such consumer distress is a significant barrier to the adoption of new technologies, which, in turn, harms commerce and discourages innovation.

Consumers Union supports the privacy and data security bills that are the focus of today's hearing. The Commercial Privacy Bill of Rights introduced by Senators Kerry and McCain puts in place some standards that would give consumers more control over their personal information. The bill's framework is rooted in a set of fair information practice principles, such as timely notice about data collection, opt-out requirements, access and accuracy requirements, and the principle of privacy by design.

We support the bill's focus on sensitive information, including information about health and religious affiliation. Companies handling such information must first get a consumer's affirmative opt-in consent. This provision would protect a young woman suffering from bulimia, for example, from having to worry that by joining an eating disorders support forum her information will be passed along to advertisers, who will market weight loss supplements to her at every step.

We also appreciate the bill's enforcement power for the FTC and state attorneys general. This will increase the likelihood that bad actors are caught and punished.

While the legislation leaves out an important foundation for better privacy practices, we also look forward to strengthening the measure so that it provides consumers with even more transparency and control. For instance, we support providing consumers with an opt-out not only for unauthorized use of covered information, but also for its collection. We'd also like to see more authority granted to the FTC to modify and update the definitions in the bill. In addition, we're concerned that the expansive language of the preemption provision could forestall state laws that seek to protect consumers beyond the intended scope of this bill.

Consumers Union also supports Chairman Rockefeller's Do-Not-Track Online Act as an important and necessary component of consumer online privacy policy. Public support for a do-not-track option is particularly high at this moment. According to the same Consumer Reports poll I mentioned before, 81 percent of respondents agreed that they should be able to permanently opt out of Internet tracking.

Some industry actors have already developed and incorporated do-not-track tools directly into browsers. Unfortunately, marketers currently can and do ignore consumers' do-not-track choices. This is precisely why Chairman Rockefeller's bill is a much needed component. Consumers Union believes that the Do-Not-Track Online Act and the Commercial Privacy Bill of Rights Act taken together

would give consumers strong privacy protections and meaningful choice in the way their information is collected and used.

Protecting consumer privacy, however, also means safeguarding data against unauthorized breaches. The Data Security and Breach Notification Act will protect consumers by requiring strong data security practices, as well as notification in case of breach. The bill will also incentivize companies to practice data minimization on the front end before a breach occurs and to provide at least 2 years of free credit reports. We are particularly pleased with the provisions that instruct information brokers to maximize the accuracy and accessibility of their records and to provide consumers with a process to dispute information.

Consumers Union would prefer that consumers be notified in any event of a breach, similar to the strongest state notice of breach laws currently in place. However, we can accept giving an exemption whenever a company demonstrates no reasonable risk of identify theft to the consumer. We urge this committee not to further weaken notification requirements.

Thank you for your time, and I would be happy to answer any questions you may have.

[The prepared statement of Ms. Rusu follows:]

PREPARED STATEMENT OF IOANA RUSU, REGULATORY COUNSEL, CONSUMERS UNION

Chairman Rockefeller, Ranking Member Hutchinson and esteemed members of the Committee. Thank you for the opportunity to appear before you today to discuss privacy and data security issues. My name is Ioana Rusu, and I am Regulatory Counsel for Consumers Union, the non-profit publisher of *Consumer Reports*® magazine.

Privacy in a Rapidly Changing World

Few can deny just how much the world has changed over the past decade. We now research and shop for products without ever leaving our homes. Our phones have become mini-computers, allowing us to organize our finances, pay bills, and order services on the go, as well as to pinpoint our exact geographical location. Social networks and online blogs enable us to create virtual lives, to reconnect with long-lost friends, and even to organize against oppressive government regimes. By transmitting and accessing more information than ever before, we've created both a vibrant online community and an efficient and convenient Internet marketplace. These incredible tools have enriched and enhanced our lives.

At the same time, however, these same tools have planted some unnerving questions in our hearts. For example, will we continue to express ourselves freely on the Internet when we know that every click and keystroke is being recorded by unknown entities, to be used for unknown purposes? And once we've entrusted our personal data to a third party, can we be sure it will it be carefully safeguarded? It is time for us to answer these questions in a clear and straightforward manner. A privacy and data security policy composed of clear, predictable, and comprehensive rules will enhance consumer trust and encourage innovation.

The first step toward this goal is our recognition that privacy is still very much a relevant and important concept in our world today. Although we live in an age of extensive sharing, very few people would agree that every piece of information they transmit should be available to everyone, for any conceivable purpose. We share information because it facilitates transactions, gives us access to services we seek, and allows us to more easily communicate with others. But it is incorrect to assume that consumers don't care about how that information is used and disseminated. In fact, in a May 2011 *Consumer Reports*® poll, 82 percent of respondents were concerned that companies they did business with may be passing on their personal information to third parties without their permission. Such consumer distrust could represent a significant barrier to the adoption of new technologies, which in turn harms commerce and discourages innovation.

Legislative Solutions for Protecting Consumer Privacy

The Commercial Privacy Bill of Rights of 2011 introduced by Senators Kerry and McCain seeks to implement some reasonable standards that would give individuals more control over who gets access to their personal information and for what purpose.

The bill's framework is firmly rooted in a set of Fair Information Practice Principles (FIPPs)—"rules of the game" that spell out how covered entities should be collecting, handling, and sharing consumer data. These principles include clear, concise, and timely notice about data collection practices; opt out requirements for certain uses of personal information; access and accuracy requirements; and the principle of "privacy by design," which requires entities to incorporate privacy protections directly into their day-to-day activities, as they develop new products and implement new technologies. Taken together, the FIPPs create a roadmap for the fair and responsible treatment of consumer data online.

We are pleased that the bill requires companies to offer consumers an opt out from unauthorized uses of their information, including the unauthorized transfer of information to third parties and the passive collection of information by third parties on first-party sites. Third-party sharing of information is extremely expansive in today's e-commerce, as tracking technologies allow advertisers to collect vast amounts of information about consumers and to aggregate them into personal profiles that are then used to target individuals much more effectively than ever before. While some consumers may not mind receiving advertising tailored to their interests, others prefer that their behaviors and preferences online remain private. The latter group should be able to choose not to have data shared with these unknown third parties.

The bill also recognizes that some types of information are more intimate and more easily used for harmful purposes than others. As a result, the bill creates a "sensitive information" category, which includes personally identifiable information (PII) that could result in physical or economic harm to an individual, or information about an individual's medical condition, medical records, or religious beliefs. If companies wish to collect, use, or share sensitive information, they must obtain the individual's affirmative opt-in consent. We strongly agree with this provision. A young woman suffering from bulimia should never worry that when she joins an eating disorder support forum, her information will be passed along to companies who will market weight loss supplements to her at every step, constantly reminding her of her obsession with her weight. She also should never have to worry that information about her condition will be sold to her insurance company, who will then raise her rates. Such uses of sensitive information are unexpected and unfair, and should not be permitted without the consumer's informed consent.

In addition, we are pleased that the bill requires entities to engage in data minimization by not collecting more data than is needed, and by only retaining collected data for a limited amount of time. Consumers Union believes that the traditional notice-and-choice approach to privacy has not done enough to allay consumers' concerns. This approach has resulted in lengthy privacy policies, filled with legalese, that consumers must "agree to" in order to access a website or receive a service. As a result, Consumers Union supports the implementation of substantive privacy principles, such as data minimization and data retention limits, which do not rely solely on consumer participation to function. These principles require companies to carry out an honest assessment of their own data practices, and to collect and retain only information necessary to the operation of their business. It is also important to note that rich repositories of information within indefinite retention periods tend to be prime targets for hackers and can expose extensive amounts of information in case of a data breach. Fewer privacy concerns will arise if only necessary data is collected and stored for a limited amount of time.

The bill grants enforcement power to both the Federal Trade Commission and state attorneys general (AGs)—a crucial provision that will increase the likelihood that bad actors are caught and punished. The enforcement provisions of the bill are crucial elements of this privacy framework, and emphasize the fact that any comprehensive privacy standards must be backed up by the force of law. The reason why industry self-regulation initiatives have largely failed to address this problem so far is that companies choose to voluntarily participate, and are held accountable insofar as they violate the stated terms in their own privacy policies. Under the proposed framework, all covered entities would be required to comply or risk enforcement action by either FTC or state AGs.

As discussed above, the Commercial Privacy Bill of Rights of 2011 lays out an important foundation for better privacy practices which Consumers Union supports. At the same time, we look forward to working toward strengthening the measure so that it provides consumers with even more transparency and control.

First of all, we support providing consumers with an opt-out not only for the unauthorized use of covered information, but also for its collection. Companies should not be permitted to amass vast quantities of information about individuals' behaviors and interests, without at least giving those individuals some notice and opportunity to opt out.

Second, we believe the bill could be strengthened by extending the definition of "sensitive information" to also include information directly tied to unique identifiers, not just to PII. As the FTC noted in its recent staff report, the distinctions between PII and non-PII are becoming increasingly irrelevant. A consumer's behavioral profile is not "anonymous" simply because it is not tied to his name or address; it is sufficient that it is tied to his particular device. Companies could use that information to treat consumers unfairly, even without access to their PII. For example, if a website does not know my name, but knows that, based on my browsing habits, I am a user with a taste for luxury goods, it could presumably show me different offers, at different prices, than it would for another user. This may result in economic harm to me.

In addition, re-identification methods today allow companies to aggregate many pieces of "anonymous" consumer information into profiles that can then be linked to actual persons. While the bill does include a provision prohibiting re-identification by third parties—a provision that we support—we believe this same prohibition should also apply to first parties who claim to collect only anonymous information from consumers. Such first parties should also be prohibited from re-identifying the consumers to whom the data applies. We are pleased to see heightened protections for sensitive information, but would like to see the definition of "sensitive information" expanded to address the ways in which online behavioral tracking is currently being carried out: though unique identifiers tied to individual devices.

Third, we wish to see more authority granted to the Federal Trade Commission to modify and update the definitions in the bill. As industry never fails to point out, this is a rapidly changing and emerging field, with new developments springing up almost on a daily basis. The FTC should have flexibility to address these new issues as they arise.

Also, the expansive language of the pre-emption provision could forestall any state laws that "relate to" covered entities' collection, use or disclosure of covered information. Although some pre-emption may be necessary to ensure uniformity in privacy practices across state lines, states should be given leeway to come up with innovative ways of protecting consumers while also supporting technological innovation. We would recommend that the pre-emption provision in the bill, at most, cover any state laws that "expressly" require covered entities to implement requirements with respect to the collection, use or disclosure of covered information. Although still preemptive, this language would be more narrowly tailored and may still allow state action in areas not covered by the bill.

While we believe the Commercial Privacy Bill of Rights Act will provide consumers with meaningful choice over how their personal information is collected, transferred, and used, our organization has long supported giving consumers the possibility to opt out of online tracking. That is why Consumers Union also strongly supports Chairman Rockefeller's Do-Not-Track Online Act of 2011 as an important and necessary component of consumer online privacy policy.

The bill would lend the force of law to industry's self-regulatory efforts by requiring that when a consumer using a Do-Not-Track (DNT) tool expresses a preference to not be tracked online, companies must respect that choice. The Federal Trade Commission would have authority to establish standards for the implementation of such DNT tools, taking into consideration the appropriate scope of such mechanisms, technical feasibility, and cost. In addition, the bill gives both FTC and state AGs authority to enforce the statute and ensuing regulations, and to seek civil penalties and damages from bad actors.

Public support for a DNT option is particularly high at the moment. According to the same *Consumer Reports*® poll mentioned above, 81 percent of respondents agreed that they should be able to permanently opt out of Internet tracking. In addition, the FTC endorsed this idea in its most recent report, and we are pleased that some industry actors have already developed and incorporated DNT tools directly into browsers. Despite the emergence of such consumer-friendly tools, however, marketers currently can and do ignore consumers' DNT choices. This is precisely why Chairman Rockefeller's bill is a much-needed component in today's privacy discussion.

Consumers Union believes that the Do-Not-Track Online Act and the Commercial Privacy Bill of Rights Act, taken together, would give consumers strong privacy protections and meaningful choice in the way their information is collected and used online.

Protecting Consumers' Data from Breaches

Protecting consumer privacy extends beyond giving consumers control over how their information is used and shared. Any comprehensive, standardized privacy policy must also address how collected information is stored and safeguarded, and what protections each consumer should enjoy in the unfortunate event of a data breach.

Last month, Sony's PlayStation network faced numerous attacks that resulted in the theft of over 100 million personal records, according to Privacy Rights Clearinghouse. And in April, the e-mail database of marketing company Epsilon was hacked and an unknown number of consumer names and e-mail addresses were stolen. Because Epsilon sends out more than 40 billion marketing e-mails annually, the potential breadth of this breach could render it the biggest of its kind in U.S. history.

The ubiquity of security breach incidents today renders the Data Security and Breach Notification Act of 2011, introduced by Senator Pryor and Chairman Rockefeller, particularly timely and relevant. Consumers Union believes this bill will protect consumers by mandating strong data security practices for all covered entities, as well as notification in case of breach. The bill will also hopefully incentivize covered entities to engage in data minimization practices on the front end, before a breach occurs.

The Data Security and Breach Notification Act first directs the Federal Trade Commission to promulgate regulations that would lay out how covered entities must maintain and protect personal information. These regulations would encourage companies to assess vulnerabilities and anticipate reasonably foreseeable attacks, in order to address those issues and prevent a breach.

If a security breach nevertheless does occur, the bill would require covered entities to provide timely notice of security breach to affected consumers and at least 2 years of free credit reports or credit monitoring. Consumers Union supports these provisions. If consumers do not know their data has been compromised, they cannot take steps to protect themselves. We also do not believe that consumers should have to bear the costs when personal information that they entrusted to a company is lost.

Although Consumers Union would prefer that consumers receive notification whenever their personal information is compromised, if there is to be a standard for risk, then Consumers Union would prefer the approach taken by this bill, where the risk is considered as an exemption rather than as an affirmative trigger. Under an "exemption" approach, a company with a security breach has to qualify for the exemption by showing that there is no reasonable risk of harm. Insufficient information about the level of risk does not eliminate the obligation to tell consumers about the breach. We would like to note, however, that the strongest state notice of breach laws do not require a finding of risk before mandating consumer notification.

We are particularly pleased that the bill focuses on the activities of information brokers, defined as commercial entities whose business is to collect, assemble, or maintain personal information concerning individuals with the purpose of selling such information to unaffiliated third parties. We strongly support the provisions instructing information brokers to maximize the accuracy and accessibility of their records, as well as to provide consumers with a process to dispute information. In addition, the provisions requiring information brokers to submit their security policies to the FTC, as well to undergo potential FTC post-breach audits, will foster accountability and enforcement of this bill.

This bill arms state officials with strong enforcement tools to ensure compliance with the law. Consumers Union agrees that state attorneys general and other officials or agencies of the State should have the authority to bring enforcement actions against any entity that engages in conduct violating the bill. State attorneys general have been at the forefront of notice of data breach issues and have played an invaluable role in addressing identity theft and data breach. Consumers' personal information will be better protected because of these enforcement tools.

Consumers Union believes that the Data Security and Breach Notification Act would encourage companies to act proactively to prevent against data breaches and to quickly address any breaches that may occur. At the same time, we look forward to working toward strengthening a couple of the provisions in the bill.

First, we are concerned that companies conducting risk assessments may not always evaluate the facts in a fair and truthful manner, in order to avoid costly notice requirements. As a result, we would suggest that companies be required to either submit the results of their self-assessments to the FTC and state AGs, or, alternatively, to maintain a copy of those results for a defined period of time and make them available to the authorities upon request. A faulty self-assessment that clearly ignores potential risks should be treated as a violation of the statute.

We also hope that the 60-day window for providing notification will be narrowed. The sooner consumers are made aware of a breach, the quicker they can take reme-

dial action. In addition, we are concerned that some credit monitoring companies are automatically billing consumers after the mandatory two free years of monitoring have ended. Consumers should affirmatively consent to any additional monitoring beyond the 2 years provided by the company.

Closing

In closing, we urge you to continue the conversation on the important topics of data privacy and security. While these three bills put in place important protections for consumer data, both online and offline, we encourage you to also consider adding additional protections for kids and adolescents. Teens between the ages of 13 and 17, in particular, make up a large portion of Internet users today. At the same time, they are more vulnerable to inappropriate uses of their personal information online. We hope you will develop some heightened standards to address the privacy of these sensitive users.

Consumers Union looks forward to working with you as these three bills move forward. Consumers are looking to you to enact standardized, mandatory and enforceable rules of the road that companies must follow when handling user data. We firmly believe that implementing these baseline principles will enhance consumer trust in the marketplace and encourage businesses to grow and innovate with confidence. Thank you for your time, and I would be happy to answer any questions you may have.

The CHAIRMAN. Thank you.

Mr. Schaaff?

Incidentally, I want to apologize to everyone about this travesty of scheduling. It's not fair to you. It's not fair to us. It's not fair to the subject. People were lined all the way down to the basement to get into this hearing. And we're all being short-changed because of votes.

We usually make one vote a day. It's usually on a judge. For some reason, now, we're going to have five votes, and it's all quite incomprehensible and totally unfair to everybody in this room.

Please proceed, sir.

STATEMENT OF TIM SCHAAFF, PRESIDENT, SONY NETWORK ENTERTAINMENT INTERNATIONAL

Mr. SCHAAFF. Thank you, Chairman Rockefeller and other distinguished members of the Committee. Thank you for this opportunity.

My name is Tim Schaaff, and I'm President of Sony Network Entertainment, a subsidiary of Sony Corporation based in California, where we employ approximately 700 people in five offices around the state. I'm chiefly responsible for the business and technical aspects of Sony's PlayStation Network and Curiosity, online services that allow consumers to access movies, television shows, music, and video games.

Sony Network Entertainment, Sony Online Entertainment, and millions of our customers were recently the victims of an increasingly common digital age crime, a cyber attack. Regarding the attack on Sony, initially anonymous, the underground group associated with last year's Wikileaks-related cyber attacks openly called for and carried out massive denial of service attacks against numerous Sony Internet sites in retaliation for Sony bringing an action in federal court to protect its intellectual property. During or shortly after those attacks, one or more highly-skilled hackers infiltrated the servers of the PlayStation Network and Sony Online Entertainment.

Sony Network Entertainment and Sony Online Entertainment have always made concerted and substantial efforts to maintain

and improve the data security systems that we utilize. We hired respected and experienced cyber security firms to enhance our defenses against the denial of service attacks threatened by anonymous. But, unfortunately, no entity can foresee every potential cyber security threat.

We have detailed for the Committee in our written testimony the time line from when we first discovered the breach, so I will not cover those details here today. However, throughout this time, we felt a keen sense of responsibility to our consumers. We shut down the networks to protect against further unauthorized activity. We notified our customers promptly when we had specific, accurate, and useful information.

We thanked our customers for their patience and loyalty and addressed their concerns arising from this breach with free identity theft protection and insurance programs for U.S. and other customers, as well as a welcome-back package of extended and free subscriptions, games, and other services. And we worked to restore our networks with stronger security to protect our customers' interests.

Let me address one of the specific issues you are considering today, notification of consumers when data breaches occur. Laws and common sense provide for companies to investigate breaches, gather the facts, and then report data losses publicly. If you reverse that order, issuing vague or speculative statements before you have specific and reliable information, you either send false alarms or so many alarms that these warnings will be ignored.

We, therefore, support balanced federal data breach legislation and look forward to working with the Committee on the particulars of the bill. By working together to enact meaningful cyber security legislation, we can limit the threat posed to all. And by simultaneously moving forward on data breach policies and legislation, we can ensure that consumers are empowered with the necessary information and tools to protect themselves from these cyber criminals.

Thank you very much.

[The prepared statement of Mr. Schaaff follows:]

PREPARED STATEMENT OF TIM SCHAAFF, PRESIDENT,
SONY NETWORK ENTERTAINMENT INTERNATIONAL

Chairman Rockefeller, Ranking Member Hutchison, and other distinguished members of the Committee, thank you for providing Sony with this opportunity to testify on cyber crime and data security.

My name is Tim Schaaff, and I am President of Sony Network Entertainment International, a subsidiary of Sony Corporation.

I am chiefly responsible for the business and technical aspects of Sony's PlayStation Network and Qriocity, online services that allow consumers to access movies, television shows, music and video games.

As you know, this year, Sony has been one of a growing number of targets of an increasingly common digital-age crime: a cyber attack.

Almost every day it seems a new story emerges about businesses, government entities, public institutions and individuals becoming victims of this cyber crime wave; thus, supporting President Obama's statement noting that these cyber attacks are "one of the most serious economic and national security threats our Nation faces." This warning was recently echoed by Defense Secretary Gates, "[t]here is a huge future threat and there is a considerable current threat [from cyber attacks]. That's just a reality we all face."

If nothing else, perhaps the frequency, audacity and harmfulness of these attacks will help encourage Congress to enact new legislation to make the Internet a safer

place for everyone to learn, enjoy entertainment and engage in commerce. We applaud this committee for its work on the issue, and we stand ready to assist you in whatever way we can.

Regarding the attack on Sony, please let me briefly provide some details, Initially, Anonymous, the underground group associated with last year's WikiLeaks-related cyber attacks, openly called for and carried out massive "denial-of-service" attacks against numerous Sony Internet sites in retaliation for Sony bringing an action in federal court to protect its intellectual property.

During or shortly after those attacks, one or more highly-skilled hackers infiltrated the servers of the PlayStation Network and Sony Online Entertainment.

Sony Network Entertainment and Sony Online Entertainment have always made concerted and substantial efforts to maintain and improve their data security systems. A well-respected and experienced cyber-security firm was retained to enhance our defenses against the denial-of-service attacks threatened by Anonymous. But unfortunately no entity—be it a mom-and-pop business, a multinational corporation, or the Federal Government—can foresee every potential cyber-security threat.

On Tuesday, April 19, 2011, our network team discovered unplanned and unusual activity taking place on four of the many servers that comprise the PlayStation Network. The network team took those four servers off line and an internal assessment began.

On Wednesday, April 20, we mobilized a larger internal team to assist in the investigation. And on that date, the team discovered the first credible indications that an intruder had been in the PlayStation Network system. We immediately shut down all of the PlayStation Network services in order to prevent additional unauthorized activity.

That same afternoon, a security firm was retained to "mirror" the servers to enable a forensic analysis. The scope and complexity of the investigation grew substantially as additional evidence about the attack developed.

On Thursday, April 21, a second recognized firm was retained to assist in the investigation.

On Friday, April 22, we notified PlayStation Network customers via a post on the PlayStation Blog that an intrusion had occurred.

By the evening of Saturday, April 23, we were able to confirm that intruders had used very sophisticated and aggressive techniques to obtain unauthorized access to the servers and hide their presence from the system administrators.

On Sunday, April 24, yet another forensic team with highly specialized skills was retained to help determine the scope of the intrusion.

By Monday, April 25, we were able to confirm the scope of the personal data that we believed had been accessed. Although there was no evidence credit card information was accessed, we could not rule out the possibility.

The very next day—Tuesday, April 26, we issued a public notice that we believed the personal information of our customers had been taken and that, while there was no—and there still is no—evidence that credit card data was taken, we could not rule out the possibility. We also posted this on our blog and began to e-mail each of our account holders directly.

On Sunday, May 1, Sony Online Entertainment, a multiplayer, online video game network, discovered that data may have been taken. On Monday, May 2, Sony Online Entertainment shut down this service and notified customers that their personal information may have been compromised.

Throughout this time, we felt a keen sense of responsibility to our customers:

- We shut down the networks to protect against further unauthorized activity;
- We notified our customers promptly when we had specific, accurate and useful information;
- We thanked our customers for their patience and loyalty and addressed their concerns arising from this breach with identity theft protection programs—at no cost to consumers—for U.S. and other customers (where available) and a "Welcome Back" package of extended and free subscriptions, games and other services; and
- We worked to restore our networks with stronger security to protect our customers' interests.

We have relaunched our networks, with stronger security protections in place, and we are pleased that our customers have been very loyal and excited about returning to them. In fact, our PlayStation Network activity level is already up to more than 90 percent of what it was before the attack. And sales of our PS3's are up double-digits this year.

Two final points. First, as frustrating as the loss of the network for playing games was for our customers, the consequences of cyber attacks against financial or defense institutions could be devastating for our economy and security. Consider the fact that defense contractor Lockheed Martin and the Oak Ridge National Laboratory, which helps the Department of Energy secure the nation's electric grid, were cyber attacked within the past several months. Even the CIA, the FBI and the U.S. Senate have recently experienced such attacks.

Second, we support federal data breach legislation that would: (1) provide consumers—regardless of what state they live in—the assurance that if and when their personal data is compromised, they will receive timely, meaningful, and accurate notice of this fact; (2) ensure that consumers receive helpful information on what measures they can take to mitigate any potential harm, including free credit reporting in cases in which such a service is warranted; and (3) treat all similarly situated companies that possess personal information equally.

By working together to enact meaningful cyber-security legislation, we can limit the threat posed to us all. We look forward to working with you to ensure that consumers, businesses and governments are empowered with the information and tools they need to protect themselves from cyber criminals. We are willing and eager to help provide law enforcement with the laws and resources they need to prevent cyber crime from occurring and bring cyber criminals to justice when prevention fails. And by simultaneously moving forward on data breach policies and legislation, we can ensure that consumers are empowered with the necessary information and tools to protect themselves from these cyber criminals.

Thank you.

The CHAIRMAN. Thank you, Mr. Schaaff.

Mr. Lenard.

STATEMENT OF THOMAS M. LENARD, PH.D., PRESIDENT AND SENIOR FELLOW, TECHNOLOGY POLICY INSTITUTE

Mr. LENARD. Thank you, Chairman Rockefeller and members of the Committee. I appreciate the opportunity to testify today.

I'd like to stress two points in my testimony: first, the importance of having reliable data and analysis for policymaking in this area; and, second, that privacy and security are different things and, therefore, should be dealt with separately. The privacy debate has engendered strong opinions but relatively little data or analysis. In order to make informed decisions, policymakers need to have facts about the practices prevalent in the marketplace. To my knowledge, the most recent systematic data on commercial website privacy practices are from 2001.

In addition to basic data, the benefits and costs of policy proposals need to be evaluated to ensure that they improve consumer welfare. For example, some proposals are likely to reduce the value of the Internet as an advertising medium both for firms and consumers and in the process reduce the revenue available to support content enjoyed by all Internet users. The principal purpose of cost-benefit analysis is to make these trade-offs explicit.

Some proposals also may not produce the intended results. For example, the idea for a do-not-track mechanism comes from the telemarketing Do-Not-Call list which has been very popular. But the effects may be quite different. The Do-Not-Call list reduces unwanted marketing solicitations. The do-not-track mechanism could have the opposite effect with consumers receiving a greater number of ads that are less well targeted to their interests.

The CHAIRMAN. Could you repeat that sentence?

Mr. LENARD. A do-not-track mechanism could have the opposite effect with consumers receiving a greater number of ads that are less well targeted to their interests.

The CHAIRMAN. OK.

Mr. LENARD. Security presents different issues than privacy. People may be quite comfortable with the intended uses of their information but worried about unintended uses and want their information to be secure. Identity theft is perhaps their primary security concern, although the most recent data show that total identity fraud in 2010 was at its lowest level in 8 years.

Regulating the collection and use of information by legitimate firms does little or nothing to deter identity theft. And, in fact, excessive control of information may increase the risk of identity theft by making it more difficult for sellers to determine if a potential buyer is fraudulent. There are two general responses to data breaches and related fraud: improved security to reduce the likelihood that such events will happen, and notification of the victims in the event that they do happen. Both are addressed in current legislative proposals.

Data breaches and identity frauds are extremely costly to the firms involved, which gives companies a very strong incentive to spend money on data security. It's, therefore, unclear that government action in this area is warranted. Incentives for notification may be less strong, and whether a regulatory notification requirement would make people better off is, therefore, an empirical question. One thing to be concerned about is that if consumers receive more notices, they may become afraid to do business online. This would be an unfortunate response because online commerce is safer than offline commerce.

Perhaps the most significant benefit of federal data security and breach notification legislation would be preempting the patchwork of state laws. For that reason, enacting a carefully crafted federal bill could yield savings for firms and consumers.

The privacy and data security debates are extremely important to the future of the digital economy and of innovation in the United States. But, unfortunately, they are taking place largely in an empirical vacuum. Without substantially better data and analysis, there's no way of knowing with any confidence whether proposals currently under consideration will improve consumer welfare or not.

Thank you.

[The prepared statement of Mr. Lenard follows:]

PREPARED STATEMENT OF THOMAS M. LENARD, PH.D.,* PRESIDENT AND SENIOR FELLOW, TECHNOLOGY POLICY INSTITUTE

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee: My name is Thomas Lenard and I am President and Senior Fellow at the Technology Policy Institute, a non-profit, non-partisan think tank that focuses on the economics of innovation, technological change, and related regulation in the United States and around the world. I appreciate the opportunity to testify before you today on privacy and data security. These issues are critically important for innovation in the digital economy, which relies on the flow of large amounts of information.

I would like to stress two points in my testimony: first, the importance of having reliable data and analysis for good policymaking in this area; and, second, that privacy and security are different and therefore should be dealt with separately.

*The views expressed here are my own and do not necessarily reflect the views of TPI, its board, or its staff.

Privacy

The privacy debate has engendered strong opinions, but relatively little data or analysis. In some respects, we had better data for policymaking 10 years ago than we do now. In 2001, when the last of a series of four studies by researchers at the FTC and elsewhere was completed, we at least had baseline data on the privacy practices of commercial websites. During the period covered by the studies, the privacy practices of commercial websites generally improved. However, to my knowledge there has been no systematic study since 2001, so no one knows what commercial website practices are today and whether they are better or worse than they were a decade ago. Policymakers can't make informed policy decisions without facts about the practices prevalent in the marketplace.

In addition to basic data, the benefits and costs of alternative privacy regimes (including the status quo) need to be carefully analyzed in order to identify the policies that will best serve the interests of consumers. The commercial use of information online produces a range of benefits, including advertising targeted to consumers' interests; advertising-supported services and content, such as free e-mail and search engines; and fraud detection and reduction in other threats, such as malware and phishing. More privacy means less information available for the marketplace and, therefore, potentially fewer benefits for consumers. Indeed, most privacy proposals are designed to make it easier for consumers to limit the amount of information firms collect and retain. The principal purpose of cost-benefit analysis is to make the tradeoffs inherent in greater privacy protection explicit and evaluate them.

On the cost side, a recent study found that the European Privacy Directive reduced the effectiveness of online advertising by about 65 percent. In other words, privacy protections make advertising less useful to consumers and, therefore, less valuable to advertisers. Advertisers will pay less for less-effective ads, which reduces the resources available to support online content. The authors found this was particularly so for more general (less product-specific) websites, such as newspapers.

Although only a few empirical studies of the costs of privacy regulation exist, even less information is available on the benefits. The benefits of privacy are the reduced harms associated with information being available or misused. If it is difficult to show harm from current practices—and thus far it has been—then it is also difficult to demonstrate that increased privacy regulation will produce benefits. We do know that people routinely give up some information about themselves in return for access to content and other services, such as e-mail and online news subscriptions, and more useful advertising. This suggests that consumers are willing to give up some privacy for the value they receive.

The benefits and costs of specific proposals, such as a Do-Not-Track mechanism should be evaluated to make sure they improve consumer welfare. Some people may use a Do-Not-Track mechanism because they derive utility simply from knowing they are not being tracked. These potential benefits need to be weighed against the costs, which include the direct costs of implementation as well as the indirect costs in terms of the quantity and quality of services and content on the Internet. Many of these costs would be borne not only by Do-Not-Track participants but by other users as well. A Do-Not-Track mechanism (depending on how many people used it) could reduce the value of the Internet as an advertising medium, and therefore the revenues available to support content for all Internet users. A Do-Not-Track mechanism could also affect the quality of major Internet services, such as search engines, which use data on search histories to update and improve their algorithms, and to protect against threats such as search spam, click-fraud, malware and phishing. The fewer data available to search engines, the less well they will perform. In sum, the information generated by online tracking generates positive externalities that support the services that everyone uses. Consumers who opted for a Do-Not-Track mechanism might be free-riding off those consumers who allowed their data to be used.[1]

The idea for a Do-Not-Track mechanism comes from the telemarketing Do-Not-Call List, which has been very popular. But the similarities between the two end at their names. People sign up for the Do-Not-Call List in order to reduce unwanted marketing solicitations. A Do-Not-Track mechanism would likely have the opposite effect. Consumers might receive a greater number of ads that are less-well targeted to their interests. This cost should also be taken into account. Several easily available tools let consumers block ads on the Internet, but a Do-Not-Track mechanism is unlikely to be one of them.

---

[1] This is in contrast to the Do-Not-Call List. Signing up for the Do-Not-Call List would not appear to impose costs on other consumers.

The three major browser providers—Google, Microsoft, and Mozilla—have announced that their products will include Do-Not-Track mechanisms. It is unclear whether this is a response to demands from consumers or to the specter of regulatory intervention. In any event, these "market" solutions should be permitted to develop without any additional pressure or requirements from the government.

Data Security

With respect to data security, the most recent survey from Javelin Strategy and Research found that total identity fraud in 2010 was at its lowest level in 8 years. While all types of fraud declined, and average costs per victim declined, mean consumer out-of-pocket costs increased, in part due to an increase in "friendly fraud"—fraud perpetrated by people known to the victim, such as a relative or a roommate.

Security presents a different set of issues than privacy. People may be comfortable with the intended uses of their data, but are worried about unintended uses and want their data to be secure. Identity theft—which involves the loss of personal data that poses a financial threat (such as a credit card number)—is perhaps the primary security concern of individuals. Regulating the collection and use of information by legitimate firms does not appear to make it more difficult for criminals to access information such as credit card numbers and, therefore, does little or nothing to deter identity theft. In fact, excessive control of information may increase the risk of identity theft by making it more difficult for sellers to determine if a potential buyer is fraudulent or not. Moreover, anything that encourages individuals to shift transactions offline is likely to be counter-productive.

There are two general responses to data breaches and related fraud—improved security to reduce the likelihood that such events will happen, and notification of the victims in the event that they do happen. Both of these are addressed in the data security bills being considered by Congress.

Substantial evidence suggests that data breaches, identity theft and related frauds are very costly to the firms involved. The FTC, in a 2003 study, found that the costs of identity theft to businesses were about 10 times the costs to individuals. Credit card issuers and merchants are typically liable for the costs of fraudulent charges—a form of insurance provided to credit card holders. The costs to firms are reflected in the significant stock market losses they suffer when victimized by security breaches. Thus, companies have a strong incentive to spend money on data security and it is unclear that government action in this area is warranted.

Incentives for notification may be less strong. However, whether a regulatory notification requirement would make people better off is an empirical question. Are the expected benefits greater than the expected costs? This is a complicated question but several factors affect how we should view notification requirements:

> First, even when consumers receive notice of a security breach, most of them do nothing about it. This lack of action is probably a rational response because even when data are compromised, the probability of identity theft is extremely small and actions like placing fraud alerts or closing accounts are not costless. Moreover, the costs of most instances of identity theft—*i.e.,* credit card fraud—are incurred by firms and not individuals.
>
> Second, we don't have good information about the range of consumer responses to notification. If consumers receive more notices, they may simply become indifferent to them. Or, they may become afraid to do business online. This would be a costly over-reaction because online commerce is safer than offline commerce. Indeed, one of Javelin's principal recommendations in its annual reports is that consumers should move their transactions online.

Because of these factors, a notification mandate should carefully target those individuals most at risk of identity fraud in order to increase its potential benefits.

Perhaps the most significant benefit of federal data security and breach notification legislation would be preempting the patchwork of state laws. Since most companies operate nationally, a state-by-state approach is unlikely to work well. For that reason, enacting a carefully crafted federal bill could yield savings for firms and consumers.

Conclusion

The privacy and data security debates are extremely important to the future of the digital economy and of innovation in the United States. Unfortunately, they are taking place largely in an empirical vacuum. Without substantially better data and analysis, there is no way of knowing with any confidence whether proposals currently under consideration will improve consumer welfare.

The CHAIRMAN. Thank you very much.

Mr. Taylor.

STATEMENT OF SCOTT TAYLOR, CHIEF PRIVACY OFFICER, HEWLETT-PACKARD COMPANY

Mr. TAYLOR. Chairman Rockefeller, members of the Committee, HP commends the Committee on its forward-looking approaches to balancing consumer privacy interests with the business realities of an Internet-based economy. I'd like to talk today about technology, trust, and privacy and how they converge to create new opportunities but also a set of challenges.

We're living in a time where our reliance on technology is ever increasing. Our business and personal lives are starting to merge. Consumers are more dependent upon mobile devices, and they have growing expectations that companies are going to be accountable stewards that respect and protect the information that we collect, that we use, and that we maintain.

HP firmly believes that our ability to succeed in the marketplace depends on earning and keeping our customers' trust. HP takes active steps to implement organizational accountability for privacy throughout our company. We believe that companies need to do more and, when asked or requested, to be able to demonstrate their capacity to uphold the obligations and the commitments that they make.

To that end, we've built an internal program that includes our privacy advisor tool, which integrates all of our commitments into a tool that helps to guide our employees. The tool looks at privacy requirements, risks, and other considerations. It helps ensure that we're able to hold every employee accountable. The concept is known as privacy by design, and it's one of the fundamental elements in the legislation that Senators Kerry and McCain have put forward that HP supports.

HP is a strong proponent of omnibus U.S. federal privacy legislation. We firmly believe that it's time for the U.S. to establish a comprehensive, flexible, legal framework that works to protect consumer privacy. We believe consumers are expecting it, businesses need it, and the economy will be better for it.

While HP also believes in effective corporate self-regulation or the possibility of innovative co-regulatory programs as outlined in the Kerry-McCain bill, the patchwork of state laws and statutes in existence today confuses customers about their protection in any given context, and it also forces companies to contend with differing and often conflicting regulations. This is why we strongly support the initiatives like Senator Pryor's data security legislation, which would set a national preemptive standard.

We believe that the adoption of new innovation depends on companies acting in an accountable and responsible manner that anticipates consumer expectations. No one is served, not corporations, not governments, and certainly not consumers, by a lack of confidence in the security and privacy of personal information. At HP, we believe that consumer trust comes from good transparency and providing meaningful choice. This is why we support the concepts in Senator Rockefeller's do-not-track legislation.

We continue to urge policymakers to examine ways to establish baseline federal legislation that will clearly articulate expectations

for all organizations. As more and more services are delivered through mobile devices, such as applications, it's going to become even more important that we have a consistent baseline standard that will strengthen that chain of accountability and unify the divergent regulations that are currently in existence.

Simply stated, HP recognizes that consumer trust is a precious commodity that must be protected through good stewardship and robust privacy programs. Federal legislation can establish a unifying federal baseline standard for organizational accountability as well as improved consumer protection. We believe that it's both a win for consumers as well as industry as a whole.

Thank you for your time, and I'm happy to answer——

The CHAIRMAN. No, thank you very much, and that was very clear and well presented.

[The prepared statement of Mr. Taylor follows:]

PREPARED STATEMENT OF SCOTT TAYLOR, CHIEF PRIVACY OFFICER, HEWLETT-PACKARD COMPANY

Chairman Rockefeller, Ranking Member Hutchison and members of the Committee, my name is Scott Taylor and I am the Chief Privacy Officer at Hewlett-Packard Company. Thank you for inviting me to testify today on privacy. HP commends the Committee for its forward-looking approaches to balancing consumer privacy interests with the business realties of a global, Internet-based economy.

We are living in a time when our reliance on technology is increasing every day. There is a continued blurring between our business and personal lives. Consumers are more dependent on mobile devices, and they have a growing expectation that companies will be accountable stewards that respect and protect the information we collect, use and maintain.

Today's technologies provide tremendous benefits to consumers and businesses and are critical to economic growth and prosperity. Yet these same innovations create new challenges related to privacy.

Privacy is a Core HP Value

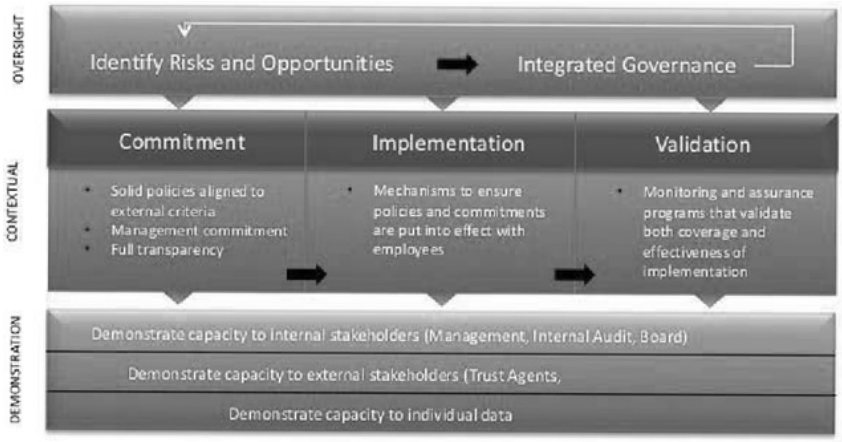
HP's core values of trust, respect and integrity provide the foundation for our commitment to privacy. HP firmly believes that our ability to succeed in the marketplace depends upon earning and keeping our customers' trust. HP has a rigorous global privacy program and is at the forefront of industry efforts to create new frameworks and strengthen privacy protections. HP takes active steps to implement organizational accountability for privacy throughout our company. We believe companies need to do more and be willing to demonstrate their capacity to uphold the obligations and commitments they make.

Accountability Framework

HP's approach to privacy is built on a model of accountability. We seek to create a chain of accountability for the information we handle, ensuring data privacy and security are advanced at every stage of the process. HP teams work together to oversee and manage our privacy efforts and collaborate with external partners to advance privacy protection worldwide.

HP's privacy accountability model is a decision-making framework that helps business units make informed choices about the risks associated with collecting and handling data. Our accountability approach demonstrates HP's commitment to privacy and goes well beyond legal compliance. Various factors are taken into consideration including first and foremost ethics as well as contractual agreements, regulations, international provisions and corporate culture. Our model builds on that foundation by considering decisions in light of our company values, customer expectations and potential risks to ensure we are fully accountable for our actions.

To that end, we have built a robust internal privacy program that focuses on integrated governance, risk and opportunity identification. Combined with strong policy commitments and senior management support, our program encourages transparency, ensures policies are instituted and validates program effectiveness. The diagram below demonstrates HP's privacy governance model:



HP monitors compliance with its privacy policies using internal assessments, customer and employee feedback, and internal audits. Our privacy team works closely with the HP Ethics and Compliance Office and internal audit function to align with their approaches to compliance. All suppliers and third-party vendors that handle HP customer and employee personal data are contractually bound to comply with applicable portions of our privacy policies and detailed supplier security standards.

Privacy and Data Protection Board

HP's Privacy and Data Protection Board (PDPB) provides company-wide oversight for privacy and personal data protection. The PDPB comprises executives from Privacy, Legal, Information Technology, Security, Internal Audit, Procurement, Internet, HP Labs, Human Resources and the Global Government Affairs functions, as well as from each business unit and region.

At quarterly meetings, the PDPB members discuss strategy and high-level priorities, assess programs, launch projects and resolve any issues identified through our ongoing monitoring programs that have been escalated to the PDPB. The PDPB regularly invites external experts to discuss privacy trends and developments. The PDPB conducts an annual risk assessment and the members work throughout the year on teams that handle specific privacy issues and mitigation projects. For example, as a result of the PDPB's work, all company laptops are required to have full-disk encryption to mitigate the risk of data theft or loss.

The PDPB enables HP to manage data protection risks comprehensively in a seamless and integrated way. Its shared risk assessment and decision-making model sets a standard for governing information management more broadly.

Privacy by Design

HP designs privacy and data protection into new products and services, guided by comprehensive, company-wide privacy standards for product and service development. This builds consumer trust and provides a competitive advantage for HP. The concept of considering privacy from inception is referred to as "Privacy by Design" and is one of the fundamental elements in the legislation of Senators Kerry and McCain that HP supports.

For corporate customers, HP's Secure Advantage portfolio offers hardware, software and services that help protect data throughout its lifecycle, whether it is stored on a desktop, laptop computer, a printer or in a data center. Privacy features incorporated into the portfolio include:

- Software that asks the user whether they want to be notified when updates are available, rather than sending notices and installing updates automatically.
- Full-disk encryption that helps protect the data on each drive, even if the disks are lost or stolen, with minimal impact on performance.
- Automated encryption devices to increase protection.

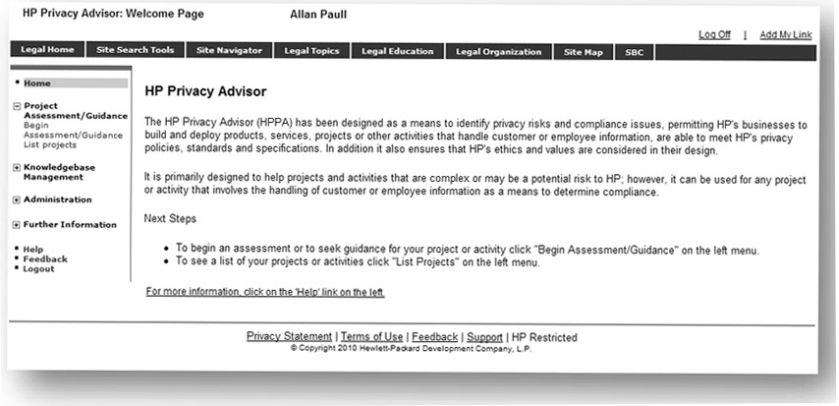
HP scientists who support our privacy team continue to work on several collaborative research projects on privacy. For example, they lead Ensuring Consent and Revocation (EnCoRe), a partnership of six organizations with the goal of making it safe and easy for people to give and withdraw consent for their data to be used.

HP scientists and engineers are working with eleven other companies on another project called Privacy and Identity Management for Community Services (PICOS) to create confidence in the safety of sharing data in online communities. Project members are identifying privacy, trust and identity management issues and plan to design and build mobile communication tools to address these issues.

Privacy Advisor Tool

Beyond our privacy team, at the core of our implementation strategy is the HP Privacy Advisor tool that integrates our privacy philosophy and commitments into an end-to-end program to better educate and guide our employees about privacy requirements, risks and considerations. This interactive tool helps to ensure that as we develop new products and services, privacy considerations are integrated from the first stages of development. Coupled with employee education and mandatory training, this tool helps to hold every employee accountable for privacy and data protection.

HP's privacy team partnered with our R&D labs to develop and deploy a Privacy by Design program to ensure that our more than 300,000 employees understand privacy implications as they conceive and develop products and programs that will collect or use personal data. Below is a screen shot that shows HP's Privacy Advisor tool:



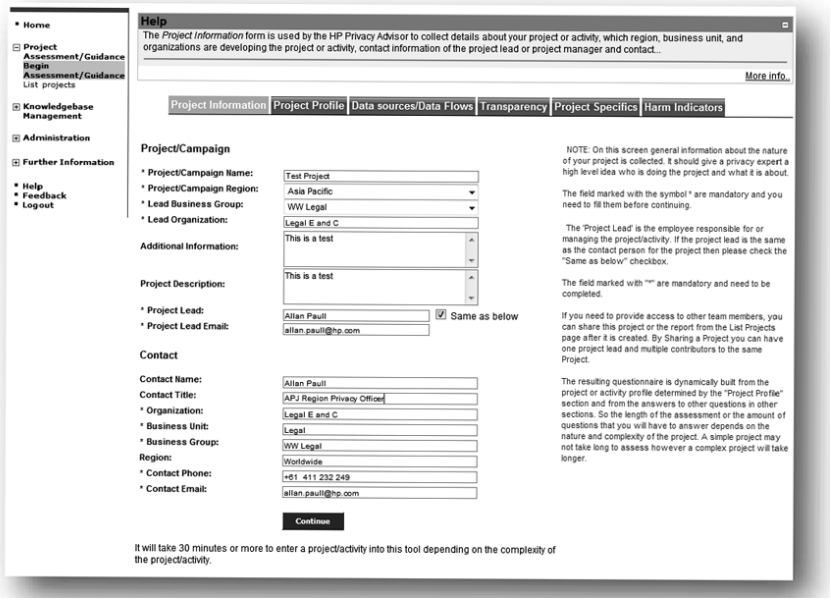
Importantly, the tool is not just about compliance. It integrates ethics and values-based considerations to ensure we align to company codes of conduct and consumer expectations. If we think about most product designers or marketing managers, they are thinking about the next innovation and their first priority isn't necessarily privacy. Whether employees are designing a new product or launching an e-mail marketing campaign, they need to understand how to put policies, obligations and values into effect. And they need to do so as they design new products and prior to deployment.

Not all innovative ideas become reality, so we need to break down product or program development into simple stages. In the design and development stages, HP's privacy team provides proactive guidance so privacy considerations can inform early planning. This has traditionally been difficult for companies and can result in a program being delayed or canceled later based on privacy concerns.

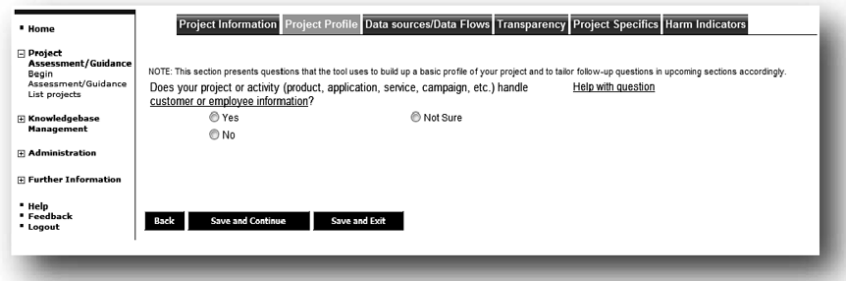
Early guidance related to privacy becomes tremendously valuable to the organization because it ensures privacy pitfalls can be avoided. In the deployment, maintenance and end-of-life stages, our privacy team does more than just guide. They provide assessment mechanisms to ensure compliance with laws, company obligations, policies and values. We have learned that this assessment needs to be as contextual as possible. For example, the way we need to assess privacy compliance in a global e-mail campaign is very different than in a new PC or web-enabled printer that seeks to deliver a customized user experience.

The HP Privacy Advisor tool is available to every employee from our internal Internet portal. Employees log in using a digital badge that authenticates their credentials and identifies them and their organization. That information is also used to assign the appropriate privacy team member for follow-up.

Here is a screen shot of the employee login page:

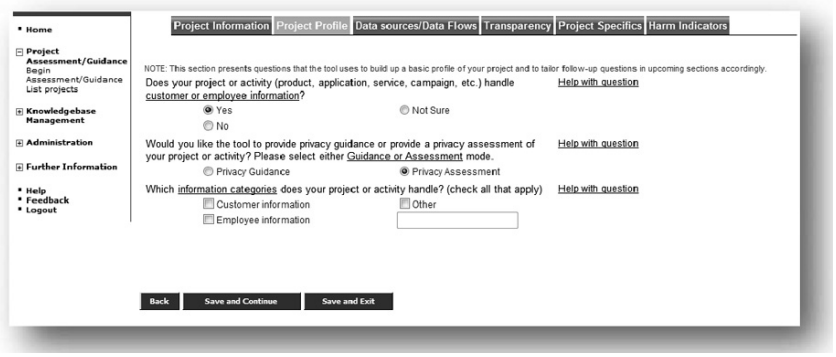


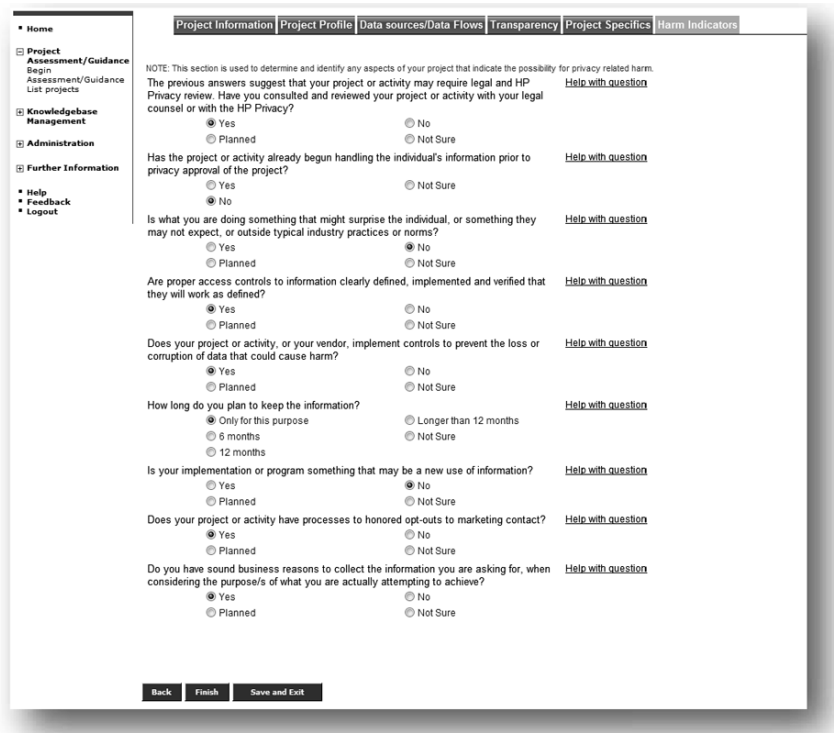
The tool starts by asking simple, basic questions about the proposed project. As each question is answered, additional dynamically-generated questions are posed based on the collective intelligence and risk factors derived from how prior questions were answered. Below is a look at sample project profile questions:



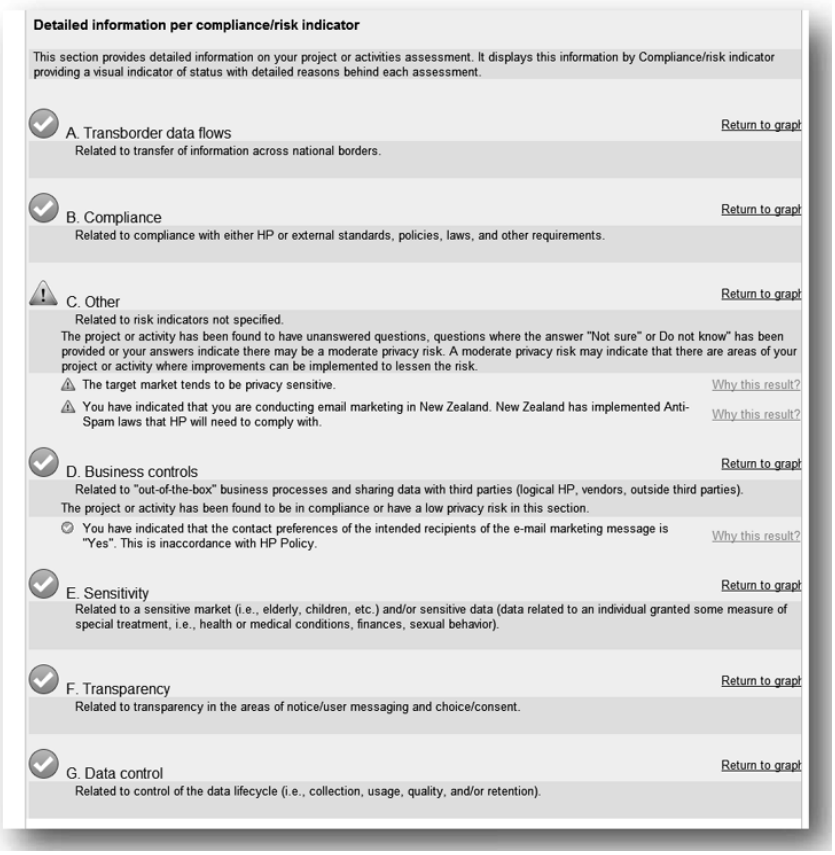
The HP Privacy Advisor tool is an intelligent privacy impact assessment mechanism that is geared to the employee user and scales from simple to complex programs. One of the greatest benefits is educating employees in the context of their program or work tasks. Through the process employees learn about privacy issues and can modify their approach to ensure compliance.

The following two graphics show additional questions based on the sample project:





The assessment results are documented and reviewed by the privacy team. Consultation is provided as necessary. If any issues exist, approval from the privacy team is required prior to deployment. After a product or program launches, triggers exist to ensure deployment was consistent with expectations and that end-of-life actions are taken when appropriate. The image below shows a report of the sample assessment results:



By using technology, we are better positioned to scale our privacy team's knowledge and guide our 300,000 employees to think about privacy in the right context and at the right time. Nothing is perfect, but we think it goes a long way to minimizing unanticipated effects, and balances our ability to innovate and ensure responsible practices when using data.

An Integrated Framework For Privacy Will Benefit Consumers

Since 2006, HP has worked closely with the U.S. Congress, the Federal Trade Commission and the U.S. Department of Commerce to establish a new strategy for federal legislation. We have long advocated for comprehensive federal privacy legislation which we believe will support business growth, promote innovation and ensure consumer trust in the use of technology. The complexity of existing state laws and statutes can make it difficult for businesses to comply with the law. We firmly believe it is time for the U.S. to establish a comprehensive, flexible and legal framework for protecting consumer privacy. Recent research from University of California, Berkeley and the Pew Research Center tells us that consumers are becoming more concerned, and increasingly want to know that their privacy is protected. We believe consumers are expecting federal legislation, companies need it and the economy will be better for it. Federal legislation would also help us compete in the global marketplace since a baseline privacy law in the U.S. allows the opportunity for international interoperability.

In addition to our work in the U.S., HP is actively engaged with Data Protection Commissioners in Europe and the Binding Corporate Rules (BCR) of our privacy program have been approved by the European Union. BCR approval is considered the highest level of certification for organizational privacy accountability. In Asia, HP helped create and shape the Asia-Pacific Economic Cooperation Cross-Border

Privacy Rules system. We are actively engaged in forward-looking frameworks in Latin America as well.

In preparation for this hearing, the Committee asked that we examine three privacy bills: (1) S. 799—The Commercial Privacy Bill of Rights Act of 2011; (2) S. 913—Do-Not-Track Online Act of 2011; and (3) S. 1207—Data Security Breach Legislation. We support the concepts espoused in all three of the bills and look forward to further collaboration with the Senate Commerce, Science and Transportation Committee, government regulators and industry to craft privacy and security laws that enable robust and rapid innovation, appropriate consumer protection, greater consistency and predictability. We look forward to continuing our engagement and furthering the efforts to increase effectiveness of the U.S. legal framework for the protection of privacy and data security. Below are our brief thoughts on each of the bills.

S. 799—The Commercial Privacy Bill of Rights Act of 2011

HP supports this innovative legislative effort by Senators Kerry and McCain. As stated earlier in the testimony, "Privacy by Design" is one of the fundamental elements in the bill and is a practice HP fully embraces. We look forward to working with Congress to advance this legislation.

Earlier this year, HP joined Microsoft, eBay and Intel in supporting the Commercial Privacy Bill of Rights Act of 2011 introduced by Senator John Kerry (D–MA) and Senator John McCain (R–AZ). Our four companies released a joint statement in support of the bill:

> We are pleased that Senator Kerry and Senator McCain, both long-time advocates for strong consumer privacy protections, have introduced the Commercial Privacy Bill of Rights Act of 2011. We support the bill and look forward to working with Congress as it moves forward.
>
> We have long advocated for comprehensive federal privacy legislation, which we believe will support business growth, promote innovation and ensure consumer trust in the use of technology. The complexity of existing privacy regulations makes it difficult for many businesses to comply with the law.
>
> We support the bill's overall framework, which is built upon the Fair Information Practices principles. We appreciate that this legislation is technology neutral and allows for flexibility to adapt to changes in technology. The bill also strikes the appropriate balance by providing businesses with the opportunity to enter into a robust self-regulatory program.
>
> We look forward to continuing our engagement to improve the effectiveness of the U.S. legal framework for the protection of privacy.

S. 913—Do-Not-Track Online Act of 2011

HP interacts with consumers and businesses in many ways online, including the sales and support of our products and services. We believe that the adoption of new innovation depends on companies acting in an accountable and responsible manner to anticipate and advance consumer needs. No one is served—not corporations, not governments and certainly not consumers—by a lack of customer confidence in the security and privacy of personal information. At HP, we believe consumer trust comes from transparency and providing meaningful choice to consumers. Accordingly, we support the concepts in Senator Rockefeller's do-not-track legislation.

With the acquisition of Palm, HP owns and operates WebOS (an operating system used in HP products). HP sells our WebOS devices configured to ensure we do not track location-based data without active user consent. When a user opts to enable location services, the data is used only for diagnostic purposes and is not shared or sold externally. Other products and services, such as our PCs, Internet-enabled printers and other mobile devices, provide similar levels of consumer transparency, choice and strong privacy protections.

We would welcome the opportunity to collaborate with Senator Rockefeller to ensure consumers are given appropriate choices for tracking in a manner that recognizes existing industry standards and technology limitations. We encourage industry to develop new standards to facilitate more meaningful choices across a consumer's online experiences.

S. 1207—Data Security Breach Legislation

Both as a consumer products company and as a service provider to other companies, HP collects and maintains personally identifiable information. Over the last 10 years, almost every state in the U.S. has adopted a data security breach law. The patchwork of state laws and statutes in existence today confuses consumers about their protections in any given context, and forces companies to contend with dif-

fering and often conflicting regulations. In some cases the laws require over-notification which does nothing to increase privacy protection. This is why we strongly support initiatives like Senator Pryor's data security legislation, which would set a single, national, preemptive standard. Such a law would create consistency and predictability for businesses and better protection for consumers.

We support the concepts and principles of the draft bill and look forward to providing input on the guidance documents. We hope to ensure that any notice required would be meaningful and useful in preventing identity theft or other related harms that may result from a data breach. In particular, notification must be prompt to enable the impacted individuals and companies to take appropriate action to protect themselves. That said, the notification time-frame must take into account the complexity and nature of the data and the breach. Moreover, the communications vehicles must be effective in reaching the intended audience and should include new media platforms when appropriate (*e.g.,* chat rooms, social media, e-mail, etc.).

Closing Statement

We continue to urge policymakers to examine ways to establish baseline federal legislation that will clearly articulate expectations for all organizations. As more and more services are delivered through multiple parties, such as applications on mobile devices, a consistent baseline standard will strengthen the chain of accountability and unify the divergent regulations currently in existence. We believe this responds to the very real needs of anxious consumers, and gives industry the flexibility to innovate in a responsible manner.

Stated simply, HP recognizes that consumer trust is a precious commodity that must be protected through good stewardship and robust privacy programs. Federal legislation can establish the baseline for organizational accountability and improved consumer protection. It's a win for both consumers and the industry as a whole.

The CHAIRMAN. I want to apologize once again. This has not been the order of what has happened. You have a committee hearing on a subject as important as this. You come from far distances, many of you, and you give your testimony.

But let me give you some solace. Actually, getting written questions from members and then you having the chance to answer them at length, or not at length, whatever your choice, sometimes works better than us asking questions.

And then, you know, the 5-minute rule messing everything up. So take some hope in that and otherwise just accept my apologies, please.

This hearing is adjourned.

[Whereupon, at 11:21 a.m., the hearing was adjourned.]

A P P E N D I X

June 29, 2011

HON. JOHN D. ROCKEFELLER IV,
Chairman,
Committee on Commerce, Science, and Transportation,
U.S. Senate,
Washington, DC.

Hon. KAY BAILEY HUTCHISON,
Ranking Member,
Committee on Commerce, Science, and Transportation,
U.S. Senate,
Washington, DC.

Dear Chairman Rockefeller and Ranking Member Hutchison:

The undersigned trade associations and business groups representing hundreds of thousands of U.S. companies from a wide variety of industry segments strongly urges caution as you examine whether changes are necessary to existing U.S. privacy law. We continue to believe that self-regulation and best business practices that are technology-neutral serve as the preferred framework for enhancing innovation, investment, and competition, while—at the same time—protecting consumers' privacy.

I. The Benefits of Data Collection and Use to the U.S. Economy

All sectors of the U.S. economy—including financial services, manufacturing, and many more—collect and use data to spur sales and job growth, enhance productivity, enable cost-savings, improve efficiency, and protect consumers. Information is used in many beneficial ways in our economy and by our society, including: fair and efficient consumer credit allocation; local and national background employment screenings and national security clearances; fraud prevention in the private-sector and in government; the collection of child support payments; and assistance to law enforcement on matters ranging from locating missing and exploited children to preventing money laundering and terrorist financing.

Businesses depend more than ever on having beneficial and trusted relationships with their customers. Better data allows businesses to deliver more relevant and targeted products and services to their existing and prospective customers. The efficient use of data allows manufacturers to reduce the cost of product development and assembly costs by up to 50 percent, and decrease the amount of required working capital by up to 7 percent.[1] Retailers utilize information for inventory control and planning, fraud prevention, marketing, and deciding where new stores should be located. The power of data helps retailers boost their profit margins by as much as 60 percent.[2]

Today, the Internet makes it possible for companies of all shapes and sizes to communicate with employees, existing customers, potential customers, and business partners around the world. The Internet, accounting for $300 billion in economic activity and over three million U.S. jobs, is clearly a key economic engine in our economy.[3] U.S. retail e-commerce sales totaled $165.4 billion in 2010, a 14.8 percent increase over 2009.[4] Frequently, online content is provided at little or no cost to consumers, and revenues are instead generated through advertising. Internet advertising revenues in the United States totaled $7.3 billion in the first quarter of 2011, representing the highest first-quarter revenue ever for the online advertising indus-

[1] McKinsey Global Institute, *Big Data—The Next Frontier for Innovation, Competition, and Productivity*, at 8, May 2011, available at: *http://www.mckinsev.com/mgi/publications/big_data/pdfs/MGI_big_data_full_report.pdf*. (McKinsey Report).

[2] *Id.* at 2.

[3] John Deighton *et al., Economic Value of the Advertising-Supported Internet Ecosystem*, June 10, 2009, at 3–4, available at *http://www.iab.net/media/file/Economic-Value-Report.pdf*.

[4] *Healthy Growth for Ecommerce as Retail Continues Shift to Web*, eMarketer Inc., Mar. 17, 2011, available at *http://www.emarketer.com/Article.aspx?R=1008284*.

try and a 23 percent increase over the same period in 2010.[5] By 2015 companies are expected to spend up to $17 billion to create and manage mobile applications related to specific products, and $38 billion in revenue are expected to be generated from consumers purchasing mobile applications for download to their smartphones and tablets.[6]

II. Self-Regulation and Best Practices Serve as Preferred Method for Safeguarding Consumer Privacy

Recognizing the importance of maintaining consumer trust in order to grow their businesses, American companies have long engaged in self-regulation to ensure that consumer privacy is protected while still allowing innovation to grow and expand our economy. Effective self-regulatory programs governing marketing and advertising have been created and implemented by many respected associations and organizations. For example, the American Advertising Federation (AAF), the American Association of Advertising Agencies (4A's), the Association of National Advertisers (ANA), the Direct Marketing Association (DMA), the Interactive Advertising Bureau (IAB), the Network Advertising Initiative (NAI), TRUSTe, the Council of Better Business Bureaus, Inc., the National Advertising Review Council (NARC), the Association for Competitive Technology, CTIA—The Wireless Association, and the Mobile Marketing Association (MMA) have been involved in the promotion of self-regulatory programs. Additionally, organizations are bound by their own privacy policies.

In the absence of any identified problem, self-regulation and best business practices continue to be the most appropriate framework for protecting consumers' privacy online while enabling innovation, investment, and competition. Self-regulatory models are a particularly effective method of protecting consumer privacy on the Internet because the regulatory process is often incapable of responding rapidly to technological changes.

III. Technology and Self-Regulation Already Offer Consumers the Type of Choice Envisioned in Recent Legislative Proposals

Recent discussion about creating a government-mandated "Do-Not-Track" list to prevent the delivery of targeted ads based on the websites that the consumer has visited provides an excellent example of the power and effectiveness of self-regulation. Companies must have the flexibility to respond to market developments and to meet changing customer needs, which a one-size-fits-all, government-mandated approach would be unable to provide.

Industry has already begun to provide consumers with the type of choice sought by proponents of a "Do-Not-Track" list. For example, the Digital Advertising Alliance—a consortium of trade associations representing more than 5,000 companies engaged in online advertising—launched a Self-Regulatory Program for Online Behavioral Advertising in October 2010, that allows consumers to opt-out from receiving interest-based ads across the Internet. Additionally, consumers using Internet Explorer, Safari, Firefox, or Google Chrome can choose preference settings that help control how their browser stores Internet usage information or the types of "cookies" that companies may set.

Any government restriction on the ability of companies to gain revenue from advertising would result in less free or subsidized content being made available to users and would inhibit innovative start-ups.

Debate over the use of location-based service (LBS) data provides another example of how consumer privacy can most quickly and effectively be protected through self-regulatory means. Smartphone and tablet users are increasingly downloading applications that offer LBS, such as navigation and mapping, the ability to locate nearby retailers, restaurants, and services, and the capability of always being connected to family and friends. Spending on LBS is expected to grow from $2.2 billion in 2009 to $12.7 billion in 2013.[7] A recent study estimates that, over the next 10 years, these services could bring $100 million in revenue to service providers and $700 billion in value to consumer and business end users.[8] Moreover, LBS-data allows wire-

---

[5] Press Release, *Internet Advertising Revenues Hit $7.3 Billion in Q1*, May 26, 2011, available at *http://www.iab.net/about__the__iab/recent__press__releases/press__release__archive/press__release/pr–052611*.

[6] Nick Bilton, *Mobile App Revenue to Reach $38 Billion by 2015, Report Predicts*, NYTimes.com, Feb. 28, 2011, available at *http://bits.blogs.nytimes.com/2011/02/28/mobile-app-revenue-to-reach–38-billion-by-2015-report-predicts/*.

[7] *San Jose Firm's Technology Helps to Find Lost Cars, Pets and More*, Silicon Valley/San Jose Business Journal, *http://www.bizjournals.com/sanjose/stories/2010/01/18/smallb3.html* (citing *Gartner, Dataquest Insight: Consumer Location-Based Services, Subscribers and Revenue Forecast, 2007–2013*).

[8] *McKinsey Report* at 85.

less carriers to manage their networks and enhance their coverage areas. This data also provides significant public safety benefits when, for example, a mobile user needs emergency assistance or roadside vehicle repair.

Policymakers have recently expressed concerns about the collection and usage of LBS data by smartphones and mobile applications. However, this is a vibrant, competitive, consumer-driven market with many groups focused on enhancing or creating new self-regulatory regimes as well as user-friendly technological solutions. For example, CTIA—The Wireless Association has developed "Best Practices and Guidelines for Location-Based Services" and a "Consumer Code for Wireless Service." The MMA has established its "Mobile Privacy Guidelines." The Association for Competitive Technology has convened a working group to develop privacy guidelines for application developers. Thus, legislation in this area is not necessary and would harm innovation, including development of the privacy-enhancing technologies that policymakers seek to foster.

IV. Data Security Legislation Would Strengthen Self-Regulation in the Privacy Area

In today's tough economy, businesses depend more than ever on having beneficial and trusted relationships with their customers. Therefore, there is no question that protecting sensitive consumer information should be a priority for all businesses that collect and store this data, and that consumers deserve to be promptly notified if a security breach has put them at significant risk of identity theft, fraud, or other harm. Thus, while self-regulation is best suited to safeguard consumer privacy, we support the enactment of meaningful federal data security legislation that does not hinder innovation or the beneficial uses of data. To be workable and effective, any such legislation must contain carefully drafted provisions, including—but not limited to—liability, federal preemption, and impact on existing federal laws.

V. Conclusion

Companies and organizations utilize a variety of effective methods—industry best practices, self-regulation, technology, and internal privacy policies—to protect consumer privacy. As you consider the need for changes to U.S. privacy law, we look forward to discussing any concerns that you or your staff may have on this issue.

Sincerely,

American Advertising Federation
American Association of Advertising Agencies
Association for Competitive Technology
Consumer Data Industry Association
CTIA—The Wireless Association
Direct Marketing Association
Electronic Retailing Association
Interactive Advertising Bureau
National Association of Professional Background Screeners
National Business Coalition on E-Commerce and Privacy
NetChoice
Network Advertising Initiative
Performance Marketing Association
U.S. Chamber of Commerce

Cc: Members of the Senate Committee on Commerce, Science, and Transportation

LISA LIBERI
Santa Fe, NM

LISA OSTELLA
Denville, NJ

June 27, 2011

NATASHA MBABAZI
Consumer Protection, Product Safety, and Insurance Staff

Senator THOMAS UDALL,
Senate Commerce Committee,

Senator FRANK LAUTENBERG,
Senate Commerce Committee,

Senator BARBARA BOXER,
Senate Commerce Committee.

Re: The Data Privacy and Security Bill Hearing, June 29, 2011—Protecting Consumers in the Modern World

Dear Natasha,

Thank you for taking the time with Lisa Liberi and Lisa Ostella. As explained over the telephone today, Lisa Ostella and Lisa Liberi have been through a complete nightmare concerning data privacy with no assistance from State and/or Federal Agencies.

Lisa Liberi was interning as a Paralegal for an Attorney in Pennsylvania. Lisa Ostella was working for a short period of time as a Webmaster for Attorney Orly Taitz. Orly Taitz resides and owns businesses in Orange County, California. Lisa Liberi spoke to Orly Taitz on one occasion in Nov. 2008; and had not met her. Lisa Liberi declined assisting Orly Taitz in her litigation against President Obama. In addition, Lisa Liberi disagreed with Orly Taitz regarding the Natural Born Citizenship laws. Lisa Ostella stopped working for Orly Taitz as a result of Orly Taitz's false law enforcement reports claiming "hacking" into her websites/PayPal Accounts and falsely accusing "Obama and his thugs." Lisa Ostella also refused to lie for Orly Taitz and refused to substantiate the false claims of "hacking." As a result, Orly Taitz targeted and came after Lisa Liberi and Lisa Ostella.

Orly Taitz stated she was going to "take down" the attorney who Lisa Liberi was interning with and to do so she was going to destroy Lisa Liberi, Orly had published all over the Internet that Lisa Liberi was the brains behind Philip J. Berg, Esquire. Destroy Lisa Liberi and Lisa Ostella she did.

Orly Taitz, as an Officer of the Court, illegally obtained background checks on Lisa Liberi and Lisa Ostella; Orly Taitz illegally obtained the credit reports and background checks of Lisa Liberi and Lisa Ostella; Orly Taitz illegally obtained medical records and sealed court records, including adoption records, of Lisa Liberi and Lisa Ostella. Lisa Liberi's credit was discussed on a radio show by Neil Sankey, the private investigator who obtained some of the private data for Orly Taitz.

Orly Taitz illegally obtained the full social security numbers; dates of birth; place of birth; mother's maiden name; children's names; father's names; addresses; phone numbers; relatives' names and addresses and other private data belonging to Lisa Liberi and Lisa Ostella and all the private primary data of Lisa Liberi and Lisa Ostella's spouses.

Lisa Liberi and Lisa Ostella's private data was obtained by Orly Taitz through third parties without any type of legal basis, permission of Mrs. Liberi and Mrs. Ostella and without any type of verification from the Reed Elsevier, Inc. companies, including but not limited to LexisNexis; ChoicePoint, Inc.; Seisint, Inc., d/b/a Accurint; and Intelius, Inc. by Orly Taitz and her private investigator's own admissions. The Reed Elsevier, Inc. companies, LexisNexis; ChoicePoint, Inc.; and Seisint, Inc. d/b/a Accurint canceled Neil Sankey, Todd Sankey and the Sankey Firm, Inc.'s Lexis accounts approximately 8 months after Orly Taitz illegally obtained Politicians private data including but not limited to President Obama and at no time investigated and/or disclosed the breach.

In turn, Orly Taitz posted all this primary identification information pertaining to Lisa Liberi all over her website located at *www.orlytaitzesq.com*; and posted the private data all over the worldwide web repeatedly; to third-party websites asking them to post it; sent out by mass e-mailing; mass mailing to Congressional individuals; to the U.S. DOJ; FBI; State and Federal entities; and sent it Internationally with Lisa Liberi's and Lisa Ostella's full Social Security number; date of birth; place of birth; mother's maiden name; father's name; address Information; and other private data, primary identification data, repeatedly for a year and a half. In fact, Lisa

Liberi's social security number is still on the Internet as of today's date at *http://www.oilforimmigration.org/facts/?p=1478* and *http://www.orlytaitzesq.com/wpcontent/uploads/2010/01/Dc279.doc*.

With this private data, Orly Taitz also began and continues cyber-stalking; Cyberbullying; cyber-harassing Lisa Liberi and Lisa Ostella, their families and children; inciting violence against Lisa Liberi and Lisa Ostella; against Lisa Liberi and Lisa Ostella. Orly Taitz called in help and harassed people in Lisa Liberi and Lisa Ostella's families and neighbors, including stalking Liberi's son; contacting people in Liberi's life for the past 25 years; sending people to Liberi's home; having people call Liberi and Ostella's home threatening their lives; filing numerous false law enforcement reports attempting to have Liberi and Ostella falsely arrested; Orly Taitz threatened to have Lisa Ostella's children professionally kidnapped; Orly Taitz was and has continued forging documents in Liberi and Ostella's name; Orly Taitz drove around New Jersey where Lisa Ostella's resided and her children attended school; Orly Taitz illegally stalked Ostella's daughter, took her picture and published the picture online; all of Lisa Ostella and Lisa Liberi's private data was sent to armed militia groups; white supremacy groups, hate groups; Lisa Liberi was called a "BLOOD red herring"; Orly Taitz illegally obtained a family photo of Lisa Liberi, her son and husband off of Liberi's computer; Taitz illegally obtained a single photo of Liberi; Liberi's pictures and home address were sent out all over the Internet, to armed militias, white supremacy groups and other hate groups, etc. These actions are still occurring as of today's date.

Unfortunately, due to the lack of privacy laws, Lisa Liberi and Lisa Ostella have been unable to get any assistance from their law enforcement agencies. An FTC Complaint was submitted to the Federal Trade Commission in or about July 2010, however, to date, Lisa Liberi and/or Lisa Liberi have been contacted.

The damages have been endless and even though Lisa Liberi and Lisa Ostella are taking civil action against Orly Taitz, she is still calling in her "cohorts" to assist her in harming Liberi and Ostella. See *Liberi, et al.,* v. *Taitz, et al.*, Case No. 8:11–cv–00485 AG, U.S. District Court, Central District of CA, Southern Division.

Lisa Liberi and her spouses identities have been stolen; their credit destroyed; Lisa Ostella's pet rabbits were slaughtered and left on her back deck; a man with a dangerous background in Albq., NM, attempted to get paid $25,000 from Orly Taitz in increments under the $10,000 reporting limits on two (2) separate occasions, which is believed to be an attempt to hire a dangerous person to harm Lisa Liberi, Lisa Ostella, their families and children, Santa Fe Police Department did not even bother to have this investigated—nor did the FBI or any other law enforcement agency. Lisa Liberi is a sitting duck for Orly Taitz and her "cohorts" to harm her, she can't move, no one would rent to her with the destruction of her credit by her and her husband's Social Security numbers and other private data being stolen and used by others due to the illegal disclosure to Orly Taitz.

This data and security bill must pass, we need laws and need all the laws to be enforced so no others go through what Lisa Liberi and Lisa Ostella have lived for the past 2–1/2 years and continue to live. We need laws so law enforcement can prosecute these crimes without jurisdictional issues and assist Mrs. Ostella and Mrs. Liberi.

There is a bunch more information regarding the breach of private data, please feel free to contact us. We will be happy to provide all the additional information and the evidence supporting the allegations herein.

Thank you,

LISA LIBERI
LISA OSTELLA

Cc: Senator Dianne Feinstein

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN D. ROCKEFELLER IV TO HON. JULIE BRILL

Question 1. Commissioner Brill, last month I asked David Vladeck why a year after the comment period had closed, the FTC had still not completed its review of the Children's Online Privacy Protection Act or COPPA Rule. Subsequent to the hearing, I was concerned to hear Chairman Leibowitz say that the FTC's COPPA proposal will not be out until the fall. I cannot understand what is taking so long. We are talking about protecting the most vulnerable Americans—kids under 13. Can you tell me why the review has not been completed?

Answer. Since we commenced our review last year, Commission staff has been diligently analyzing the public comments in connection with the review. This work involves a wide range of complex issues, and requires thorough consideration of

technical topics and privacy concerns. At the same time, we have continued to enforce the existing Rule, most recently announcing a $3 million settlement with Playdom, Inc., and we will announce several additional COPPA settlements shortly. The internal work on the COPPA Rule is nearly complete, and I expect that the Commission will publicly release the findings soon.

Question 2. Will you commit to me that you will work with the other Commissioners to update the rule as quickly as possible?

Answer. Yes, of course. I am committed to our work in this area, and the privacy issues affecting our children have my full attention. I will continue to work with the other Commissioners and Commission staff to release the findings and update the Rule as quickly as possible.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. CLAIRE MCCASKILL TO HON. JULIE BRILL

Question. The United States may need a national framework to ensure that personal data remains secure in an increasingly electronic world and to mitigate harm in the event of a breach. As we consider legislation, it is important that we do not end up with a patchwork of federal data security laws, with multiple regulations from multiple federal agencies. That doesn't help consumers and could create competitive disparities that could distort the marketplace and create confusion. Do you agree that it is not productive to have multiple agencies with authority over the same parties, creating possible duplication of efforts and confusion and disparities for consumers and businesses?

Answer. I certainly agree that strong federal data security and breach notification legislative requirements are critical. The Commission has testified before Congress in support of such legislation. Overlapping regulations from multiple federal agencies could create confusion and we would be pleased to work with Committee staff to reduce or eliminate any such overlap.

As Congress continues to consider legislation, we will continue—as we have done in the past—to work cooperatively with our sister agencies to avoid duplicative or redundant oversight. For example, the FTC and FCC cooperated successfully several years ago in "pretexting" cases. These cases involved individuals who pretended to be the owners of telephone accounts. Under these false pretenses, they obtained the calling records for these accounts from telephone companies and sold the records to others. The FTC took action against entities involved in such pretexting, and the FCC focused on ensuring that telephone carriers had ample security in place for calling records. Our collective goal in these collaborative efforts is to ensure that there are no gaps that would leave consumers unprotected.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN F. KERRY TO HON. JULIE BRILL

Question 1. Commissioner Brill, can you describe the nature of the harm that consumers experience due to the insufficiency of the privacy frameworks currently in place in the United States?

Answer. The insufficiency of the privacy frameworks currently employed in the United States have resulted in considerable harms that may have been avoided had certain privacy protections, as outlined in the FTC's staff privacy report been in place.

For example, in 2002, the Commission entered into a consent order with Eli Lilly and Company resolving allegations that it publicly disclosed e-mail addresses of subscribers to an e-mail reminder service relating to an anti-depressant drug manufactured by the company. Certain privacy protections, including an emphasis on privacy by design (as recommended in the FTC staff privacy report), may have avoided this incident, which unquestionably harmed consumers by publicly disclosing sensitive health-related information.

More recently, the Commission entered into a consent order with Google Inc., resolving allegations that, in connection with the launch of its social media product, Google Buzz, the private contacts of consumers were made public by default in certain cases. By disclosing private e-mail contacts, Google Buzz may have revealed the identities of those individuals and organizations that consumers were in contact with, including attorneys, health providers, professional recruiters, etc. The disclosure of this type of information could lead to certain conclusions being drawn by others that can negatively impact consumers. For example, the fact that a consumer is in contact with a particular medical provider could suggest that he is suffering

from a sensitive medical condition. Similarly, the fact that a consumer is communicating with a professional recruiter may lead others to conclude he is job hunting. Again, as in the incident involving Eli Lilly and Company, had Google built certain privacy protections into its operations, this type of harm may have been avoided.

Both of these cases involved allegations of deception under section 5 of the FTC Act, because the companies had made certain promises to consumers about their information practices. Had the companies not made these claims, however, we may not have been able to address these incidents. Moreover, currently there is no general legal requirement for companies to disclose their privacy practices, and recent evidence exists that companies in the rapidly expanding mobile application field, for example, do not. The Future of Privacy Forum think tank analyzed the top 30 paid applications at the end of May 2011, and discovered that 22 of them lacked even a basic privacy policy.

Another recent example of unexpected and potentially harmful information use involves efforts by insurance companies to use data collected online to predict disease and insurance risk. Media reports indicate that this may occur without the consumer's knowledge or an opportunity to contest the findings. Basic privacy protections, such as clear disclosure and adequate choice up front, would allow consumers to protect themselves in these situations.

The potential for harm exists with other types of information as well. For example, consumers have historically relied on state and federal law protections governing disclosure of the books they check out of the library and their video rental history, but these protections may not reach all the reading or viewing activities of consumers as they simply browse the web. If this information were linked to individual consumers, it could be used to make judgments about political affiliation, sexual orientation, or other sensitive issues. Another example of harm we explored in our privacy roundtables involves "sucker lists." Consumers can find themselves on marketing lists targeted to sensitive medical conditions or impulsive purchasing behavior. These lists can facilitate efforts to take advantage of vulnerable consumers.

Question 2. Commissioner Brill, technology is far more powerful and capable of data collection and distribution than it was even 10 years ago. How do technological advances such as context awareness (devices being able to tell what you are doing and who you are with) and data aggregation impact the framework of existing privacy models?

Answer. As we learned in our series of public roundtables, existing privacy models have not kept up with these types of changes in technology. For example, a pure notice-and-choice model that relies on lengthy privacy policies has proved unworkable and now, in an era of small screens, even less feasible. Consumers should not have to scroll through dozens or hundreds of screens to understand how companies collect, use, and share their data.

Similarly, a model that only addresses quantifiable harms associated with misuse of data may not address the full range of consumers' privacy concerns. For example, as you point out, advances in technology have enhanced companies' ability to store and aggregate consumers' data and use it in ways not understood, intended, or disclosed at the time of collection. Moreover, context aware devices may allow companies and others to draw conclusions about consumers that were not previously possible. Entities that can track the location of an individual using a Smartphone could discern, for example, that the individual spends considerable time at an address catering to addiction treatment, or in the vicinity of a municipal building that houses the probation office.

Question 3. Commissioner Brill, some critics of both the recommendations the FTC has made to industry and the legislation that I and other members have introduced is that we do not know enough about collection practices and uses to make privacy standards necessary. I believe that we know what constitutes fair information practice principles and we know that a significant portion of collectors of information do not comply with them. I think we should have a law that requires them to do so and have proposed one. How do you respond to the criticism that neither the FTC nor Congress knows enough to establish baseline rules for how people's information is collected, used, and distributed?

Answer. I don't agree with this criticism. I believe that policymakers have sufficient knowledge of industry practices to encourage certain bedrock principles. The Commission has been examining the issues surrounding online privacy for years—since at least the mid-1990s. During the three Commission privacy roundtables held in 2009–2010, we heard from hundreds of participants from academia, consumer groups, industry, trade associations and others. I believe we have a considerable understanding of how industry is collecting, using and disclosing information about consumers. Because industry will continue to innovate, my goal is to develop uni-

versal principles that will continue to be relevant regardless of how industry progresses. These principles, including privacy by design, simplified choice and improved transparency, are ones that can be applicable in nearly all situations, and there appears to be widespread agreement that companies should be implementing these principles.

Question 4. Commissioner Brill, data brokers deal in the acquisition of information from an original source of collection to share with other unrelated entities who might want to use that information. I have two questions for you as it relates to data brokers and their practices:

Should companies be able to buy from and sell data to data brokers, without the consent of the consumers that are the subject of that data?

Answer. The Commission staff's report supported the idea that companies should provide consumers with meaningful choice before sharing their data with third parties, including data brokers. Our staff report also supported the idea that consumers should have reasonable access to information data brokers maintain about them, and in appropriate cases, the right to correct this information or have it suppressed. Further, the report noted the extent of access and the consumers' ability to correct or suppress information should be scalable to the sensitivity of the data and the nature of its use. I fully support these proposals.

Question 4a. If consumers did not consent to collection by a data broker and do not have access to or the right of correction regarding erroneous data gathered about them without their permission, how can the government help data brokers eliminate erroneous data and protect consumers?

Answer. If data brokers sell information for credit, employment, insurance, housing or other similar purposes, they must provide certain protections under the Fair Credit Reporting Act ("FCRA"). For example, they must take reasonable steps to ensure accuracy of the information they sell and they must inform purchasers of their obligation to provide adverse action notices to consumers. Even when the FCRA is not applicable, the FTC staff report proposed that data brokers provide consumers with reasonable access to information maintained about them, and in appropriate cases, the right to correct this information. I support this proposal.

Question 5. Commissioner Brill, the FTC made its first call for comprehensive privacy protection under a Democratic majority in 1999. This FTC issued a draft report calling for privacy by design, simpler more streamlined choices for consumers, and transparency in data collection practices and uses last year. As you know, we modeled our legislation on that report and witnesses on the next panel will speak directly to the legislation. Do you have a sense of the proportion of collectors of information that are not today incorporating privacy protections into the design of their services or meeting the other baseline fair information practices you lay out?

Answer. Although we do not have statistical information of that nature, based on our investigations and general policy initiatives, it is evident that many companies are still lagging in incorporating basic data security standards in their everyday practices. We have also seen evidence that privacy disclosures are not being used by a substantial numbers of mobile applications ("apps"). Recently, the Future of Privacy Forum think tank analyzed the top 30 paid apps and discovered that 22 of them lacked even a basic privacy policy. It is clear that work remains to be done in order to achieve widespread compliance with basic privacy protections.

Question 6. Have you had a chance to review the legislation and in your analysis, to what extent does it meet the three recommendations for policymakers included in the draft report?

Answer. I am pleased to see that basic privacy protections like those laid out in our FTC staff report—such as privacy by design, improved notices, and increased transparency—are incorporated into the draft legislation. I believe it would be useful for Commission staff to continue to discuss the draft legislation with your staff.

Question 7. In our legislation, we are calling for comprehensive protections that allow people to opt out of having their information collected for uses they should not have to expect and beyond that, we arguing that we also need other rules, like the ability to have consumers ask firms to cease using their information if they lose trust in that company as well as the knowledge that companies are required to have accountability and security measures in place before they collect people's information.

You have said that prior approaches to privacy protection focused solely on threats to harm after the harm has occurred or relied on simple notice of collection, and that efforts to offer choice of whether or not to have that information secured have fallen short. If you believe that the "no harm, no foul" and simple notice and choice solutions are inadequate as I do, would you not agree that we need a new comprehensive privacy law?

Answer. I agree that we need a new approach to consumer privacy. The Commission staff embarked on its privacy reassessment and issued its preliminary privacy report in recognition of the inadequacies of existing approaches to consumer privacy. I also agree that companies should follow basic privacy principles like those laid out in the staff report. As you know, however, the Commission has not yet taken a position on legislation.

Question 8. Commissioner Brill, in a May 4 speech you gave, you responded to the criticism that a Do Not Track option would dry up advertising revenue. You said that "As the Commission learned during our discussions and research prior to issuing our report, when given an informed and more granular choice, most consumers, including myself, want to receive tailored ads—and will choose to share information for that purpose."

I agree with that, which is why although we require collectors to give consumers a choice about whether their information is collected or not, we did not make a universal choice mechanism the centerpiece of our legislation. Given that you think most people will not opt-out of having their information collected, are not the other fair information practice principles—security of information, clear and specific notice, ability to access data or call for cessation of its use, and the requirement that data be collected and held only as long as necessary, to name a few—just as important or more important than whether or not we can secure a universal do not track choice?

Answer. I agree that comprehensive privacy protections are very important. The protections that are reflected in your bill, including data security, privacy by design, and clear notices, are critical to ensuring basic privacy protections. Do Not Track can be a very effective tool for consumers to exercise choices about the growing industry practice of behavioral advertising. Do Not Track will not address other current privacy concerns.

Question 9. Commissioner Brill, the FTC report calls for different treatment for first-party collectors of information and third-party collectors. It is a concept we adopted in our legislation as well because we believe a first-party interaction is known to the consumer and some degree of trust is implicit. Could you explain the difference in your mind and why different treatment is warranted?

Answer. The Commission staff report recognizes that the relationship that consumers have with first parties is different from the relationship they have with third parties. When a consumer goes directly to a retailer's website to obtain a product or service, the consumer inherently understands that she is sharing information with that retailer. However, when visiting that retailer's website, the consumer does not understand or expect that the retailer will be sharing her information with other companies ("third parties"). That is why our staff report recommended that consumers be given clear notice and choice about such information sharing with third parties. This distinction, however, must be drawn carefully. If first parties are defined broadly to include Internet Service Providers ("ISPs") or other companies that have access to almost all consumers' browsing behavior, then consumers would likely have a different expectation about the use of their data by those companies than they would a typical retailer. Consumers would undoubtedly be surprised, and may in fact be concerned, to learn that ISPs or similarly situated companies could use all of their browsing behavior without their consent. For this reason, the staff report noted that enhanced consent or even more heightened restrictions would likely be warranted for practices such as ISPs' use of Deep Packet Inspection to create marketing profiles.

Response to Written Questions Submitted by Hon. Barbara Boxer to Hon. Julie Brill

Question 1. In your written testimony, you note that the FTC has brought 34 data security cases during the past 15 years. During this same period of time, state Attorneys General have been free to file cases under state law to protect their citizens. What has been your working relationship with state Attorneys General on data security matters, and has their ability to prosecute state laws ever conflicted or hindered the FTC's prosecution of its cases?

Question 2. Have the efforts of state Attorneys General assisted the FTC in its enforcement of consumer privacy and data security laws?

Answers 1 and 2. The FTC has a history of working well with state Attorneys General on enforcement actions in many types of cases. Having served for many years in state Attorneys General offices, I can say from experience that the Commis-

sion has worked well with the state AGs. The agency's continued commitment to this cooperation is among my top priorities.

Commission staff engaged in privacy and data security-related investigations regularly interact with staff from the state AGs and enforcement actions are coordinated when appropriate. For example, in the enforcement action involving LifeLock—a company that provided an identity theft prevention service—35 states joined the Commission, together obtaining a $12 million settlement involving charges that it used false claims to promote its services.

As we do with our sister federal agencies, we work closely with state AGs to prevent any conflicting or duplicative enforcement actions.

Question 3. I am concerned about the effect of the data breach bill's preemption of California law. As you may know, California law requires a company to notify consumers of a breach if there is a reasonable belief that personal information was accessed without authorization. Do you have an opinion on whether it is best for data breach notification to be triggered on whether there has been unauthorized access to data, or whether notification should be triggered on a company's determination as to whether there is a risk of harm?

Answer. There may be a risk that requiring notification any time there has been unauthorized access to data could result in over-notification to consumers, causing them to ignore the important notices. Therefore, generally, it may be useful to have companies make an objective reasonable determination as to whether the breach will not pose a reasonable risk of harm. In such cases, a notice would not be required.

At the same time, however, for certain sensitive data, unauthorized access to such data may create a presumption of harm. For example, in the Commission's Health Breach Notification Rule, the Commission stated that, because of the sensitivity of health information, unauthorized access would be presumed to create a risk of harm.

Question 4. In *AT&T* v. *Concepcion*, the U.S. Supreme Court ruled that federal arbitration law preempts California law banning the use of class action waivers in consumer agreements. Some professors and consumer advocates in California have expressed concern that this decision could have an effect on state data breach laws, such as the strong law in effect in California. Do you believe the Supreme Court's decision could have an impact on states' ability to pass strong consumer protection laws, particularly in the data breach/notification area?

Answer. I note that the California state data breach law contains a private right of action. Cal. Civ. Code §1798.84. Under the decision in *AT&T* v. *Concepcion,* it appears that companies handling consumer data could mandate in their consumer agreements that consumers address any problem related to data security and notification through individual arbitration.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. MARK BEGICH TO HON. JULIE BRILL

Question. Besides passing legislation is there anything else that can be done to assist consumers' digital education so they have a better understanding of the consequences of their online and offline data profiles?

Answer. As we mentioned in the December 2010 preliminary staff privacy report, we believe that all stakeholders should work to educate consumers on privacy issues, particularly in the digital world. For its part, the FTC has a very active program to educate families about steps people can take to protect their data online, and understand how companies may track their online activity. Many school systems have ordered materials from the FTC, or adapted them for their own use. We encourage schools that aren't yet using these materials to consider sharing them with teachers, parents and students.

Since October 2009, the FTC has distributed over eight million copies of the guide for parents, "Net Cetera: Chatting with Kids About Being Online." Approximately 20,000 schools, school systems, law enforcers and other community organizations have placed orders. The Net Cetera guide helps adults lead a conversation with kids about online privacy and safety, rather than taking a lecturing approach.

Recently, *OnGuardOnline.gov* released a new publication designed to educate consumers about mobile apps, "Understanding Mobile Apps: Questions and Answers." The guide explains what apps are, the types of data they can collect and share, and why some apps collect geolocation information. The FTC issued the guide to help consumers better understand the privacy and security implications of using mobile apps before downloading them.

In September 2011, the FTC will release a revamped *OnGuardOnline.gov* site, in coordination with the Department of Homeland Security's Stop.Think.Connect campaign. The site, which will feature a blog, will continue to be the Federal Government's site to help users be safe, secure and responsible online.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KELLY AYOTTE TO HON. JULIE BRILL

Question 1. In a May 2011 interview, Chairman Leibowitz stated that "one of the Commission's priorities is to find a pure Section 5 case under unfair methods of competition. Everyone acknowledges that Congress gave us much more jurisdiction than just antitrust." However, in 2009, the U.S. Chamber of Commerce published an article that casts doubt on the FTC's authority to expand its jurisdiction under Section 5. The Chamber stated, "The character of many of these proposals, as well as their scope and diversity, highlights key disadvantages of extending Section 5 beyond the range of the existing antitrust laws." Do you agree with the Chamber's views that we should look with skepticism at the expansion of Section 5? If not, why not?

Answer. Congress established the Commission as a bipartisan independent agency with a mandate to protect the public from unfair methods of competition. Congress intended that the Commission play a unique role in the economic life of the nation. As the Supreme Court explained in *FTC* v. *Sperry & Hutchinson Co.*, 405 U.S. 233, 239 (1972), in which it thoroughly examined the legislative history of the FTC Act, Congress intended for the Commission to proscribe unfair business practices that are not condemned under the letter of the antitrust laws. Senator Cummins (R. Iowa), one of the main sponsors of the bill establishing the FTC, squarely stated on the Senate floor: "[t]hat is the only purpose of Section 5 to make some things punishable, to prevent some things, that can not be punished or prevented under the antitrust law." 51 Cong. Rec. 12,454 (1914). While the vast majority of our antitrust enforcement actions involve conduct that falls within the prohibitions of the Sherman or Clayton Acts, the Commission has a broader mandate, which it discharges by challenging, under Section 5, conduct that is likely to result in demonstrated harm to consumers or to the competitive process.

Indeed, Section 5 may be the only practicable means to stop harmful conduct that cannot be reached under the antitrust laws. The Commission's recent use of Section 5 demonstrates that the Commission is committed to using that authority in predictable ways that enhance consumer welfare. For instance, the Commission used Section 5 in the recent U-Haul settlement to prevent "invitations to collude" by fixing prices. A competitor's invitation to its nominal rival to fix prices does not violate the Sherman Act, but it serves no lawful purpose and creates an intolerable risk that price fixing will result. And even if an invitation to collude is rejected, it can undermine the process by which prices are set by independent competitors and lead to tacit coordination. In the article you mention, the Chamber of Commerce "acknowledge[s] that there are certain, limited forms of anticompetitive conduct that may not be covered by the antitrust laws," including invitations to collude.

Congress chose to give the Commission its broad mandate rather than handing the Commission a list of specific acts to be condemned as unfair because it knew that no such list could be, or long remain, sufficiently complete to protect competition and consumers. To address concerns about the fairness of not doing so, Congress limited the remedies available for violations of Section 5. The Commission is limited to certain remedies, such as cease and desist orders, to stop harmful conduct; the agency cannot seek a fine or civil penalty as a result of a Section 5 violation. Moreover, Section 5 of the FTC Act does not provide for a private right of action, and no party may obtain treble damages under the FTC Act.

Because of the limited consequences of Section 5 enforcement, the Commission uses its Section 5 authority not to punish the wrongdoer, but to fairly eliminate the conduct that is likely to injure competition and consumers, allowing honest and competitive markets to further consumer welfare.

Question 2. The Association for Competitive Technology represents a number of tech companies including Microsoft, Oracle, and VeriSign. ACT has blogged about Chairman Leibowitz's desire to expand the FTC's Section 5 authority. It wrote that Chairman Leibowitz "is arguing that requiring actual economic analysis of alleged "harms to competition" is too high a bar for his agency. They need to be able to prevent business practices they believe are harmful to competition and consumers, even if the economic analysis suggests otherwise. And in this new regime, companies will have little guidance as to what the FTC will consider legal vs. illegal." This doesn't

seem to be the right policy for the agency to be pursuing. Why is the FTC doing so?

Answer. The Commission will not bring a case where the evidence shows no actual or likely harm to competition or consumers. As the Chairman explained in his testimony before the Senate Judiciary Committee last summer, "Of course, in using our Section 5 authority the Commission will focus on bringing cases where there is clear harm to the competitive process and to consumers." That is, any case the Commission brings under the broader authority of Section 5 will be based on demonstrable harm to consumers or competition. As the Second Circuit held in the *Ethyl* case,[1] there must be some "indicia of oppressiveness" before the FTC can bring an enforcement action under Section 5. We have adhered to this standard in our cases. For instance, in the recent Intel case, the Commission alleged that Intel's behavior harmed consumers and the competitive process in a number of ways, such as raising the price of computers; limiting consumer choice; inhibiting competition from non-Intel chip makers; reducing innovation by computer makers; and reducing the quality of industry benchmarking. Commission staff was prepared to offer proof of these harmful effects to establish that Intel violated Section 5, as well as Section 2 of the Sherman Act. Intel offered to settle the case, resulting in a Commission order eliminating the harmful conduct.

Question 3. Prior to Google's announcement of an FTC investigation into its competitive practices there were a lot of news stories about the battle between the FTC and the DoJ over which agency would get to investigate the company. In fact, Assistant Attorney General for Antitrust Christine Varney questioned whether two agencies should have antitrust review powers. She stated, "I would leave to Congress how they would like to resolve the overlapping and sometimes inconsistent jurisdiction between the agencies . . . I think what business does need is clarity, certainty and understanding of the legal framework within which their deals will be evaluated." Do you think that the overlapping jurisdictions of the FTC and Department of Justice—and the fights that they produce—are a good thing for American businesses and consumers? If not, how would you propose to fix it?

Answer. I believe the FTC and the Department of Justice work well together to promote and protect competition and the interests of American consumers and businesses. Both agencies have areas of expertise, and the differences in their organizational structures are quite deliberate and provide certain benefits. For example, the FTC was created by Congress as an independent agency with expertise in both consumer protection and antitrust. One of the principal benefits of the FTC is that it is bipartisan and our decisions require consultation and consensus. That means that our enforcement efforts remain relatively consistent as we go from Administration to Administration. Further, because Congress wisely charged the Commission with competition and consumer protection enforcement, we have a broad perspective that enhances our work. The FTC also was chartered by Congress to employ non-enforcement tools, such as issuing reports, performing empirical studies, and advocating for pro-competition reforms with other government agencies, to support and strengthen the agency's competition and consumer protection missions.

This year, the agencies worked closely together on several joint policy projects to provide transparency and predictability for businesses subject to the antitrust laws. Last August, FTC and DOJ issued revised Horizontal Merger Guidelines, a core document that provides businesses with a clear view into how the agencies conduct antitrust merger reviews. This year, the agencies also jointly developed a Proposed Antitrust Enforcement Policy relating to cooperation among health care providers organizing Accountable Care Organizations under the new Patient Protection and Affordable Care Act. These joint statements reflect a high level of consensus and cooperation, and serve as models for competition agencies throughout the world.

It is true that there are occasional clearance disputes over which agency is in the better position to investigate a matter. In most instances, one or the other agency has greater expertise in the industry of potential concern due to a previous investigation, and clearance is given to that agency right away. But in grey areas, such as where neither agency has conducted an investigation in the past, both agencies can make a claim that a related investigation gives them a head start on the facts and issues that are likely to arise. The FTC and DOJ have a process in place to resolve clearance disputes, which helps resolve the issue quickly, so that one agency can get started on the investigation and minimize any burden on the parties. Recently, clearance disputes have been rare and are handled quickly.

---

[1] *E.I du Pont de Nemours & Co.* v. *FTC,* 729 F.2d 128 (2d Cir. 1984) ("Ethyl").

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN F. KERRY TO HON. CAMERON F. KERRY

Question 1. General Counsel Kerry, I understand that you have had discussions with our trading partners in Europe, Asia, and the Americas on privacy. I get the sense that our disagreements with them are more about form than substance. That is, we share values but not a common platform of law. Could you talk about what is going on in the rest of the world on this issue and how you and Congress can participate in that dialogue effectively?

Answer. Privacy is a deeply held value in America, reflecting long-standing legal, political, and cultural traditions. Our laws express this value. Respect for privacy is broadly enshrined within the Bill of Rights, most dramatically in the Fourth Amendment. Privacy protections are woven into the fabric of our common law and state laws. Congress has further protected various types of information about individuals through legislation aimed at specific industries or categories of information, such as health, finance, education, and information about children. Some of the companies that operate in these targeted industries have adopted multi-stakeholder-created codes of conduct which are enforced by the Federal Trade Commission (FTC) and by state Attorneys General. Between legislation and these codes of conduct, there is strong protection for information about individuals in these specific sectors.

Other countries have adopted different models. With the advent of Internet commerce, several multinational bodies developed comprehensive data privacy models that draw nearly all data privacy contexts under a single legal framework. In large part, these laws are grounded in the internationally recognized Fair Information Practice Principles that were originally created by the United States Department of Health, Education and Welfare back in 1973. In 1995, for example, the European Union (EU) passed its Data Protection Directive (DPD), which provides an EU-wide, omnibus framework focused on these fair information principles. Similarly, the Organization for Economic Cooperation and Development (OECD) has issued Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, and the Asia Pacific Economic Cooperation has issued a Privacy Framework, which also enshrine the Fair Information Practice Principles. Many member countries have implemented this framework in their own national laws, including Argentina, Australia, Canada, India, Japan, Mexico, South Korea, and all 27 member countries of the EU. These laws are generally applicable to information about individuals irrespective of the industry in which the information is obtained.

Because key American players in the Internet, including online advertisers, cloud computing service providers, providers of location-based services, and social networking sites, operate in sectors without specific statutory obligations to protect information about individuals, much of the information about individuals currently traversing the Internet fall into these "gaps" in commercial privacy legislation. This has led to a misperception in some foreign quarters that the United States does not have strong privacy protections and does not care about privacy.

Even though the United States does not have a unitary legal framework in the private sector that governs commercial data privacy, our system of protections is strong and actively enforced by the FTC, by agencies that regulate in specific sectors, and by the States. Furthermore, there is an expanding corps of privacy professionals in the United States dedicated to considering privacy issues and complying with privacy regulations, both domestic and foreign. As the data protection commissioner of another country said to me at an international conference of data protection and privacy professionals: "My colleagues tell me the Americans have no respect for privacy, but how come all the people who attend these conferences are American?" Many recognize that the flexible regime of U.S. privacy laws has facilitated innovation and contributed to development of some of the world's most advanced online services.

The European Union is currently revising its Data Protection Directive, and we are concerned this may result in changes that would restrict cross-border data flows. In our engagement with the EU, its member states, and other international partners, my Administration colleagues and I are working toward minimizing multiple compliance burdens and giving businesses and consumers consistent rules and expectations.

The most important thing Congress can do is to enact baseline privacy protection to make American commercial data privacy law comprehensive, creating protections that would apply to all businesses in the absence of more specific industry legislation. The Administration has issued a call for enacting such protections in the form of a consumer privacy bill of rights based on the Fair Information Practice Principles our country pioneered long ago. The EU is closely watching our pending privacy-related legislation. If Congress were to enact comprehensive commercial data

privacy legislation that fills in the gaps in consumer protections, this would demonstrate renewed U.S. leadership in privacy protection and help prevent fragmentation of the Internet that becomes a barrier to the cross-border free flow of information essential to the United States and to global trade and commerce.

Question 1a. How many other members of the OECD have a general law of privacy for commerce based on the Fair Information Practice Principles?

Answer. Within the OECD, 32 of the 34 members have a general commercial privacy law based on the Fair Information Practice Principles—all members except the United States and Turkey.

Question 2. GC Kerry, we are talking about both privacy and what happens to people's information when security fails. How would a privacy framework based on the Fair Information Practices impact data breaches (*i.e.,* only retaining the data for as long as needed, implementing good data security, privacy by design, etc?)

Answer. The premise underlying the Administration's proposal for federal security breach notification legislation is that creating greater transparency and accountability through breach reporting will improve the state of data security practices. The Administration's security breach notification proposal does not recommend any specific set of data security requirements.

Other Administration and Department of Commerce proposals contain recommendations to improve security for digital information, including but not limited to information about individuals. In the context of consumer data privacy legislation, the Administration recommends an approach based on a comprehensive set of Fair Information Practice Principles (FIPPs). Widespread implementation of such principles could help address some of the conditions that lead to security breaches. For example, observing the principle of data minimization—collecting only the information about individuals that is needed and securely deleting or disposing of it after it is no longer needed—could lead firms to collect less information about individuals that could be subject to unauthorized disclosure. This principle would, of course, need to be implemented in such a way that it did not hamper the ability of law enforcement to continue to ensure public safety. Similarly, a "privacy by design" approach could lead to the collection of less information about individuals and to the incorporation of technical and organizational approaches to keeping it secure.

Question 3. GC Kerry, in the Department of Commerce report issued last year, your agency did not call for a Do-Not-Track option to go in to law. Can you talk about the pros and cons of Do-Not-Track proposals and its role as a part of the larger privacy framework we should be considering?

Answer. Although it is premature to comment on specific Do-Not-Track proposals currently being debated, the Administration believes that Do-Not-Track is exactly the type of complex subject that would benefit from the multi-stakeholder process outlined in our response to Question 5, where stakeholders with different interests and perspectives would work together toward agreement on an enforceable code of conduct for the industry. Such a process would allow industry to be responsive to changing consumer expectations and rapidly-changing technology without the need for additional legislation.

The FTC's current work on Do-Not-Track embraces this model, and I applaud the leadership of Chairman Leibowitz, as well as browser developers, privacy advocates, and others, to provide options for greater control over personal information.

Question 4. GC Kerry, the FTC and the FCC both have a role in privacy oversight today. Senator McCain and I are proposing consolidating that oversight under the FTC to the degree that activities telephone and cable companies undertake in collecting information are already covered by another law. Again, this remains a work in progress and we are open to alternative constructions of the bill. Given that cable and telephone companies are collecting information for the same business reasons as any other market actor, is there a good reason to govern them under different agencies or under different constraints?

Answer. Generally speaking, the Internet Policy Task Force Green Paper and other Administration statements have recommended keeping existing sector-specific federal data privacy statutes in place and avoiding duplicative regulation. We will consider this issue further as we develop the Administration's proposal.

Question 5. GC Kerry, in our legislation we include a safe harbor program by which industry can work cooperatively with regulators to construct procedures for adherence to fair information practice principles that are workable and effective. Could you talk to the concept of the multi-stakeholder cooperative process and how you think it could work?

Answer. Multi-stakeholder processes are not an untested idea. Groups such as the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C) have used transparent, consensus-driven processes to set a wide range of

Internet-related technical standards. These processes have been successful, in part, because stakeholders share an interest in solving the underlying challenges. Today the standards for basic Internet communications protocols that support trillions of dollars in global commerce each year are developed through these consensus-driven processes.

The 1990s Internet policy framework began with a series of multi-stakeholder events and forums that informed policy and prompted self-regulatory action. Major websites agreed to post privacy policies, the nascent online advertising industry developed a code of conduct, and the FTC enforced adherence to these voluntary practices.

The Administration believes that the flexibility provided by well-crafted multi-stakeholder processes offers the most effective solution to the challenges posed by a rapidly changing technological, economic, and social environment. We need a process that is nimble enough to enable stakeholders to respond quickly to consumer data privacy issues emerging from new technologies and business practices without the need for additional legislation.

The two key characteristics of a successful multi-stakeholder process for a wide variety of privacy challenges—including data security, and Do-Not-Track—are legitimacy and flexibility.

Legitimacy means that the broad array of stakeholders affected by consumer data privacy have a chance to be heard—and actually are heard. The process we envision will put industry leaders at the table alongside consumers, privacy advocates, state regulators, academics and appropriate federal agencies. We want to engage all of them in a dialogue about how to guarantee the privacy consumers have a right to expect, while enabling businesses to develop new technologies, products, and services, and meeting legitimate public safety concerns and other important public interests.

Flexibility ensures that the process continues to adapt to changes in technology and services in the digital economy. The issues will touch on technology, business needs, individual values, U.S. law, and international law and policy among many other things. The process needs to accommodate these different, changing considerations.

We see a need for our government to take the initiative to convene stakeholder discussions. We are convinced that Executive Branch involvement as a facilitator will inject energy, legitimacy, and urgency to get stakeholders moving.

The Department of Commerce will initiate the process by working with private sector stakeholders, consumer groups, privacy advocates, and government partners, to identify specific arenas where privacy practices are unclear and clear rules would benefit consumers and businesses. Once convened, these stakeholders will hold the pen when drafting the codes. The end goal is to produce an enforceable code of conduct that meets FTC approval.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. MARK BEGICH TO HON. CAMERON F. KERRY

Question. Besides passing legislation is there anything else that can be done to assist consumers' digital education so they have a better understanding of the consequences of their online and offline data profiles?

Answer. As technologies mature, consumers will naturally become more educated in the privacy issues related to those technologies. However, there are certain actions Congress and the Administration can take that will help speed up that constantly-evolving process.

Congressional hearings on commercial data privacy have helped raise awareness of data privacy practices. Forums convened by agencies like the Department of Commerce and the Federal Trade Commission have also increased awareness and interest in the issues surrounding consumers' data profiles. There are also many privacy conferences that explore these issues and help educate privacy professionals, who in turn help educate an increasingly sophisticated population of consumers.

We will continue to engage with the private sector as conveners, speakers, participants, and listeners at privacy conferences. We will also continue leading initiatives like the National Strategy for Trusted Identities in Cyberspace, which is focused on enhancing consumers' convenience, security, and privacy in online transactions, and the National Initiative for Cybersecurity Education, which has as one of its three strategic goals to raise awareness about the risks of online activities. This kind of leadership and participation has sped-up the production of tools that provide consumers more awareness and control over their online data profiles, such as browser Do-Not-Track tools and privacy architecture.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. CLAIRE MCCASKILL TO AUSTIN C. SCHLICK

Question. The United States may need a national framework to ensure that personal data remains secure in an increasingly electronic world and to mitigate harm in the event of a breach. As we consider legislation, it is important that we do not end up with a patchwork of federal data security laws, with multiple regulations from multiple federal agencies. That doesn't help consumers and could create competitive disparities that could distort the marketplace and create confusion. Do you agree that it is not productive to have multiple agencies with authority over the same parties, creating possible duplication of efforts and confusion and disparities for consumers and businesses?

Answer. A uniform and consistent set of privacy and data security standards employed consistently across government could protect consumers and provide certainty to companies that handle personal data. These standards would not, however, preclude sector-specific privacy regimes overseen by experienced expert agencies. In particular, different types of consumer data may warrant different treatment, and the same type of information might warrant different treatment by companies in different industries. For example, an individual's health-related information may raise different concerns than the same individual's consumer spending-related information, and overseeing data security with respect to these different types of data may be most successfully done by the agencies that have expertise and experience with the industries and types of data at issue.

The FCC, for instance, has extensive experience protecting consumers through the agency's authority over the privacy practices of communications providers. Section 222 of the Communications Act requires telecommunications carriers to safeguard information about, for example, the numbers consumers dial, the length of time they spend using the network, and their location when they use wired or wireless services to make calls. Over the years, the Commission has responded to evolving technologies and networks by promulgating increasingly protective rules to safeguard consumers' privacy. Our network-focused privacy and data security rules are sound, settled, and legally tested. Sections 338 and 631 of the Communications Act also protect personal information. These provisions establish requirements for satellite and cable television providers' treatment of their subscribers' personally identifiable information, including information about the extent of any viewing or other use by the subscriber of a cable or satellite service or other service provided by the cable or satellite operator. The requirements include clear and conspicuous notice about collection and use of subscribers' personal data, limiting disclosure of personal data, and remedies for subscribers who suffer a violation of these provisions.

The FCC also has experience with successful collaboration in areas of overlapping agency jurisdiction. Working in parallel with the FTC, the FCC adopted "Do-Not-Call" regulations under Section 227 of the Communications Act. The FCC and the FTC also collaborated on implementation of the CAN–SPAM Act, with the FCC adopting rules that prohibit sending unwanted commercial e-mail messages to wireless accounts without prior permission. The FCC and the Department of Justice enforce Section 705 of the Communications Act, which prohibits unauthorized interception of radio communications and unauthorized disclosures of wire or radio communications.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. MARK BEGICH TO AUSTIN C. SCHLICK

Question. Besides passing legislation is there anything else that can be done to assist consumers' digital education so they have a better understanding of the consequences of their online and offline data profiles?

Answer. Consumer education is an ongoing priority for the FCC, particularly in the area of privacy and data security. The National Broadband Plan specifically recognized the importance of educating consumers about the potential consequences of their online profiles and helping them manage those profiles in a manner that maximizes the privacy and security of the information.

The Commission's E-rate program also requires that any school receiving E-rate funding for Internet access or internal connections must have an Internet safety policy. At Congress's direction, we are implementing a new requirement for 2012 that those policies must provide for educating minors—at the school's discretion—about appropriate online behavior.

The FCC also participates in numerous consumer education initiatives across the Federal Government in the area of privacy and data security. The FCC is an active participant in OnGuard Online, a website sponsored by several government and pri-

vate organizations that helps consumers guard against fraud and identity theft on the Internet. The FCC also is part of the public/private National Initiative for Cybersecurity Education partnership that encourages sound cybersecurity practices, including protection of consumers' online profiles. The FCC will continue to support these and other initiatives that educate consumers about the importance of protecting their online identities.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN D. ROCKEFELLER IV TO STUART K. PRATT

Question 1. Mr. Pratt, while your testimony focuses on use of information by data brokers for fraud prevention, law enforcement and child protection, the industry is much broader than that. According to news reports, consumer information is collected, aggregated, and sold by data brokers for marketing and other purposes. To provide a fuller record, please provide the following:

- A comprehensive list of data brokers and the types of consumer information they collect by entity, how the data is acquired, how it is aggregated, and how it is marketed to potential buyers.

Answer. There may be companies that produce valuable products for American businesses who want to reach customers and which fall under the definition of the term data broker as your bill defines it. However, CDIA does not represent these types of companies and cannot answer for them. CDIA is an international trade association with more than 190 member companies, providing our nation's businesses with the data tools necessary to manage risk in a wide range of consumer transactions. These products include credit and mortgage reports, identity verification tools, law enforcement investigative products, fraudulent check transaction identification systems, employment screening, tenant screening, depository account opening tools, decision sciences technologies, locator services and collections. Our members' data and the products and services based on it ensure that consumers benefit from fair and safe transactions, broader competition and access to a market which is innovative and focused on their needs. We estimate that the industry's products are used to manage risk in more than nine billion transactions per year. The sources of data used to develop these products vary. Examples of sources include financial institutions, insurance companies, retailers, public records, utilities companies, telecommunications companies and consumers, themselves.

Question 1a. A detailed and comprehensive list of the types of entities purchasing data from data brokers and the types of information and purpose for purchasing such information.

Answer. The users of risk-management products produce by our members will vary. We include a range of uses in our testimony. Examples include insurance companies, financial institutions of all types, law enforcement agencies, government entitlement program providers, federal, state and local government administrative and regulatory agencies, retail merchants, public and private universities, non-profit organizations, collection agencies, child support enforcement programs and agencies, centers for missing and exploited children, retailers, healthcare providers and more.

The specific purposes for purchasing the data for risk management will vary. Some purchase data to verify consumers' identities in order to prevent identity theft and to comply with federal laws and regulations relating to this crime such as Section 326 of the USA Patriot Act or FACT Act Red Flags Rules. Others will purchase data to make sure that the consumer with whom they are doing business has the ability to pay for the product or that the premium is set fairly relative to the risk. An online retailer or government agency may purchase data to ensure that addresses to which packages or mailings are sent to the most up-to-date address and not to fraudulent addresses. Child support enforcement agencies and those which focus on missing and exploited children use location and investigative data tools to enforce orders and to prevent child abuse.

Question 1b. Your understanding of what existing laws cover, if any, the collection, maintenance, and transfer or sale of each type of information described in your responses to the requests above.

Answer. With regard to CDIA's members there are numerous laws at the federal and state level that regulate the collection, maintenance, and transfer or sale of information, including but not limited to:

- The Federal Fair Credit Reporting Act (FCRA) as well as various state Fair Credit Reporting Acts;
- Title V of the Gramm-Leach-Bliley Act (GLBA);

- The Drivers Privacy Protection Act (DPPA);
- The Health Insurance Portability and Accountability Act (HIPAA);
- The Children's Online Privacy Protection Act (COPPA);
- The FTC's Do Not Call list;
- The Fair Debt Collection Practices Act;
- Section 5 of the FTC Act and similar state UDAP Statutes;
- Equal Credit Opportunity Act;
- The CAN–SPAM Act;
- The Telemarketing Consumer Protection Act; and
- Numerous state data protection/data security/data breach notification laws.

Question 2. Mr. Pratt, you suggest the data broker provision in Senator Pryor's and my bill will undermine law enforcement and fraud prevention even though our bill makes an explicit accommodation for "governmental, child protection, and fraud prevention purposes." Given this exemption, why do you believe the bill would undermine those efforts?

Answer. As suggested in our oral remarks offered at your hearing, it is our view that the committee has a tremendous opportunity to pass new law establishing a national standard for ensuring the security of sensitive personal information and ensuring that consumers are notified when the loss of sensitive personal information poses a significant risk of identity theft. CDIA continues to support the enactment of an administratively-enforced national standard for both concepts.

With regard to the information broker provision consider the following specific concerns which are drawn from our September 22, 2010 testimony offered at a legislative hearing on S. 3742, the Data Security and Breach Notification Act of 2010 and which remain in this version of that legislation, as well.

Interference with Fraud Prevention, Identity Protection and Location Services—RVI products such as those designed for fraud prevention and location are produced under laws such as the Gramm-Leach-Bliley Act and Section 5 of the Federal Trade Commission Act.

The definition of information broker does not exclude financial institutions regulated under GLB. Therefore products developed under the data-use limitations found in GLB Title V, Section 502(e) are adversely affected by the information broker provision. Neither a product developed for fraud prevention nor location should be subject to accuracy, access and correction standards since neither product is used to deny or approve an application, etc. If they were designed for the purpose of making decisions about a consumer's eligibility, then they would already be regulated under the FCRA.

Consider the effect of the information broker duties on fraud tools. While Section 2(b)(3)(A)(ii) provides a limited exception for fraud data bases consisting of inaccurate information, the exception is not sufficient, though we do applaud the effort to try and address the problem of imposing an accuracy standard on fraud tools. Fraud prevention tools are built based on data about confirmed fraud attempts, data about combinations of accurate and in accurate data used for fraud attempts and more. Fraud tools are designed to identify transactions or applications that are likely to be fraudulent in order to allow the user to take additional steps to prevent the crime and still process legitimate transactions. The current exception does not appear to address all types of fraud prevention tools used today and further the limitations of the exception impose statutory rigidity that will prevent the design of new tools as the strategies of the criminals change. It is our view that applying an accuracy standard to any aspect of a fraud prevention system that is not used to stop a transaction or used to make a yes-or-no decision does not make sense.

Similarly it is wrong to subject fraud prevention tools to an access and correction regime. While Section 2(b)(3)(iv) attempts to exclude fraud prevention tools from the duty to disclose (and therefore any right to dispute data), the exception is tied to a variety of tests such as where the use of the tool would be "compromised by such access." It is our view that fraud tools, because they are not used to make decisions, should be absolutely excluded from duties to disclose. If details of a fraud tool are disclosed it is akin to disclosing the recipe for fraud prevention. The fact that the exception to disclosure is not absolute leaves open the risk that a tool will have to be disclosed which simply reduces the value of fraud prevention tools which are protecting consumers. This result works against the premise of the bill which is to protect consumers from crime, particularly identity theft.

As discussed in this testimony, location services are materially important to how risk is managed. These tools are not designed to be used for decisionmaking and thus are not regulated under the FCRA, which already regulates all data used for

eligibility decisions (including the imposition of accuracy, access and correction rights). Location services cannot have an accuracy standard applied to them as this bill would propose. The tools are about helping local law enforcement investigate crimes, attorneys to locate witnesses, and federal agencies to cross match data in the pursuit of kidnappers, etc., nonprofit hospitals to collect debts from patients who have the ability to pay but refuse to do so and in the enforcement of child support orders. These systems are designed to, for example, help a user identify possible connections between disparate records and ultimately possible locations for the subject of the search. Measuring the quality of the possible connections is not akin to an accuracy standard, nor should an accuracy standard be applied to "possible matches." Further, providing access to a database for purposes of error correction could affect the quality of the systems since matches are sometimes based on combinations of accurate and inaccurate data. Ultimately, the data is not used to deny a consumer access to goods or services and thus CDIA opposes the application of accuracy, access and correction duties to these fraud prevention systems or RVI services."

Thank you for this opportunity to add to your hearing record.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. ROGER F. WICKER TO STUART K. PRATT

Question. Mr. Pratt, in your testimony, you cite the litany of current laws aimed at data security and protecting consumers' personal information, such as the Gramm-Leach-Bliley Act and HIPAA. Further, you caution against creating "overlapping burdens" where companies are already in compliance with security and notification standards for sensitive personal information. As we explore this issue, how can we ensure creating a national standard will not overlap with these laws and create additional burdens on industry?

Answer. It's our firm belief that one very definite way to eliminate some statutory and regulatory overlap as well as to avoid misapplication of data management principles is to eliminate the "data broker" provisions from the bill entirely. In doing this the Senate Commerce Committee can focus on the tremendous opportunity to move a bill that will establish an administratively-enforced national standard for securing sensitive personal information and notifying consumers when the loss of sensitive personal information poses a significant risk of identity theft.

Another specific step you can take is to ensure that where a person is already subject to a duty established by other federal law, regulation or agency guidance to secure sensitive personal information or to notify consumers where the loss of sensitive personal information poses a significant risk of identity theft, that the person is deemed in compliance with the proposed bill's duties. While there are some exceptions included in the bill, they are incomplete because the bill proposes that entities must be "in compliance with" and not merely "subject to" these duties. By adopting this "in compliance with" test, the current bill essentially requires all U.S. businesses that are subject to both laws to comply with both laws, since falling out of compliance with one leads to being out of compliance with both. This is entirely the wrong result, and CDIA urges the Committee to strike this test in favor of a simple set of exceptions tied to a "subject to" standard.

Finally, the bill must establish a "field preemption" standard which applies to all entities who are either subject to the bill or who are deemed in compliance with the bill. This type of preemption ensures that states cannot alter or affect in any way the operation of the national standards for data security and breach notification. If preemption is not perfected then the bill will result in persons still being subject to new or slightly altered state laws.

We are happy to provide your staff with amendatory language for each of the concerns outlined above.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. JOHN D. ROCKEFELLER IV TO IOANA RUSU

Question. What types of consumer information is currently being collected by data brokers, for what purposes, and is there adequate transparency for consumers? Would the data broker provisions in the Data Security and Breach Notification Act give consumers greater protections than existing law?

Answer. One significant problem associated with data collection activities carried out by many information brokers is that few people know exactly what types of information are being collected, and how they are being used. Consumers often do not even realize that these brokers exist, much less that they are collecting information

about consumer behavior which can then be used to alter important outcomes for individuals.

Nevertheless, there have been some reports and investigations into the activities of these companies. For example, a recent Washington Post article entitled, "*Little-Known Firms Tracking Data Used in Credit Scores*" [1] detailed the activities of what it called the "fourth bureau:" private companies that compile and sell consumer data to entities such as lenders, landlords, employers and health-care providers. Unlike the three major credit bureaus, which track consumer scores based on credit card activity, auto notes and mortgages, the fourth bureau tracks and investigates traditionally unreliable indicators of creditworthiness, such as magazine and cable subscriptions, utility bills, and child care tuition payments. The Fair Credit Reporting Act sets standards for handling of credit information, but it does not necessarily cover all the activities of the "fourth bureau," and enforcement of this law has been spotty.

Most American consumers have no way of knowing that this information is being collected about them and used in ways that could affect their interest rates, housing, and employment. Even when individuals find out about the "fourth bureau's" existence, accessing and correcting data about them can be very difficult. Consumers Union submitted a letter last week to both Senate and House Commerce and Banking Committees, asking that Congress investigate the activities of these entities and address concerns surrounding consumer privacy and FCRA compliance.

In addition, in its December 2010 staff report, the Federal Trade Commission acknowledged that information brokers currently have the ability to collect and aggregate data from a wide variety of online and offline sources, as well as public and private sources. Data brokers may, for example, contract with retailers to acquire consumer purchase information.[2] Some also maintain lists of individuals that are considered particularly susceptible to certain marketing campaigns or scams.[3] Data brokers can use collected information for a variety of purposes, including providing identity verification services to third-parties. Information thus obtained, whether correct or erroneous, could be used to deny individuals access to funds, admission to an event, or membership in a group. Such uses may fall outside of the FCRA, thus depriving consumers of the protections offered by the Act.[4]

Because data brokers do not interact directly with consumers, they often do not notify consumers when data is being collected. Many also do not provide consumers with some means to opt out of the collection. As noted in the FTC report, the most troublesome aspect of this business is that it is invisible to consumers, and allows the aggregation of massive amounts of information about them into consumer profiles that can be used for a variety of unanticipated purposes. Such secret dossiers pose significant privacy concerns.

The information broker provisions in S. 1207 would impose standardized, mandatory requirements on these companies. Under the bill, information brokers would have to provide consumer access to collected information, as well as a process for consumers to dispute and correct erroneous information. Data brokers would also have to maximize accuracy of collected information. In addition, the bill prohibits information brokers from engaging in pre-texting in order to obtain consumer information. These provisions would provide consumers with greater protections than those currently existing in law, because they would cover entities that may not technically fit into the traditional FCRA definitions. Those companies have often argued that they are not subject to FCRA. This bill would ensure that even in situations where FCRA does not apply, information brokers still grant consumers access to information about them, and make reasonable efforts to ensure information is accurate.

As this legislation moves forward, we hope your Committee will also consider strengthening the information broker section by including a requirement that whenever an entity uses information furnished by these brokers to make an adverse decision about a consumer, that consumer must receive notification. Access and correction rights are certainly important. However, if a consumer does not know that bro-

---

[1] Ylan Q. Mui, "Little-Known Firms Tracking Data Used in Credit Scores," *Washington Post*, July 16, 2011, available on the web at: *http://www.washingtonpost.com/business/economy/little-known-firms-tracking-data-used-in-credit-scores/2011/05/24/gIQAXHcWII_story.html*.

[2] Fed. Trade Comm'n, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers," (2010) (preliminary FTC staff report), available at *http://www.ftc.gov/os/2010/12/101201privacyreport.pdf*.

[3] *Id.* at 31, referencing *Written Comment of Chris Jay Hoofnagle, University of California, Berkeley School of Law*, cmt. #544506–00012, at 5 (quoting Karen Blumenthal, "How Banks, Marketers Aid Scams," *Wall St. J.*, July 1, 2009).

[4] *Id.* at 74, note 171.

kers are collecting and selling personal information about them, they will have no way of knowing they should access and correct erroneous data.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BARBARA BOXER TO IOANA RUSU

Question 1. As you know, California was the first state to enact data breach and notification laws in 2002, which became effective in 2003. California has been a leader in the area of data breach laws, and has continued to pass laws enhancing protections for consumers since the initial law. However, I am concerned about the state law preemption provisions in S. 913 (Kerry-McCain privacy bill) and S. 1207 (Pryor-Rockefeller data security bill), which would prevent California enacting laws in the future to deal with new threats to consumers. Do you believe that leading states such as California should be preempted from improving their consumer protection laws?

Answer. Consumers Union supports the idea that states should be "laboratories of democracy," constantly evaluating existing law and proposing new solutions for rising issues. Our organization supported the California breach law passed in 2003 and we have a long history of working with state legislatures to pass initiatives that would protect consumers. As a result, we would certainly prefer that any federal law addressing data breach and notification set out a floor, not a ceiling, allowing states to innovate and address new threats to consumers.

However, we are also concerned that the current patchwork of state notification rules may prove unworkable in the long run. We believe that the pre-emption language currently included in S. 1207 is narrowly drawn.

In addition, we are also particularly concerned about the activities of information brokers. Too often, consumers have no idea that these hidden entities are tracking their behavior and collecting information about them from online and offline sources, which is then aggregated and used to create comprehensive consumer profiles. We believe that the provisions of the bill, which would require access, accuracy, and a process for consumers to dispute and correct erroneous information, would go a long way toward bringing more transparency to the activities of these data tracking companies. As a result, although Consumers Union would prefer that the bill not preempt state initiatives, we believe that the overall bill would increase protections of consumer data.

Question 2. As you may know, California law requires a company to notify consumers of a breach if there is a reasonable belief that personal information was accessed without authorization. However, this law would be preempted by S. 1207. Do you have an opinion on whether it is best for data breach notification to be triggered on whether there has been unauthorized access to data, or whether notification should be triggered on a company's determination as to whether there is a risk of harm?

Answer. In testimony to Congress on this matter, Consumers Union has repeatedly pointed out that the strongest state notice of breach laws do not require a finding of risk before mandating consumer notification. Although Consumers Union would prefer that consumers receive notification whenever their personal information is compromised, if there is to be a standard for risk, then Consumers Union would prefer the approach taken by this bill, where the risk is considered as an exemption rather than as an affirmative trigger. Under an "exemption" approach, a company with a security breach has to qualify for the exemption by showing that there is no reasonable risk of harm. Insufficient information about the level of risk does not eliminate the obligation to tell consumers about the breach.

Question 3. Do you believe that state Attorneys General play a vital role in the enforcement of consumer laws, such as data security and privacy laws?

Answer. Consumers Union strongly believes that state Attorneys General must be involved in the enforcement of consumer laws such as S. 1207. State attorneys general have been at the forefront of notice of data breach issues and have played an invaluable role in addressing identity theft and data breach. With more cops on the beat, consumers' personal information will be better protected.

Question 4. In *AT&T* v. *Concepcion*, the U.S. Supreme Court ruled that federal arbitration law preempts California law banning the use of class action waivers in consumer agreements. Some professors and consumer advocates in California have expressed concern that this decision could have an effect on state data breach laws, such as the strong law in effect in California. Do you believe the Supreme Court's decision could have an impact on states' ability to pass strong consumer protection laws, particularly in the data breach/notification area?

Answer. Consumers Union is troubled by the U.S. Supreme Court's finding in *AT&T* v. *Concepcion*. The Court's decision to strike down the California law in question appears to allow companies to draft contracts that legally bar consumers from obtaining redress through class-action lawsuits or even group arbitration. Consumers Union believes that class actions and group arbitration represent important tools for consumers to challenge companies that have wronged them, particularly in cases where many consumers have suffered relatively small economic harms. As a result, we are concerned that under this ruling, strong state consumer laws may be nullified by provisions buried in consumer contracts.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CLAIRE MCCASKILL TO TIM SCHAAFF

Question 1. In reviewing proposals that address data security, it is important that Congress learns more from industry sectors about how they are dealing with these issues. How has the hacking incident of 77 million of your customers' accounts affected your business and approach to data breach?

Answer. The hacking incident led us to take action that significantly disrupted my company's network business and our consumers' use of our services, and, for the entire industry, these illegal attacks highlighted the widespread problem of cyber security. To protect our network and our consumers from online hackers, we felt compelled to shut down our services. We worked hard to restore the services and to keep our customers informed. We asked our customer for their patience and understanding. We have been rewarded with a strong return of our customers to our network. Since coming back online there has been a net increase of approximately 3 million new user accounts. Following the attacks, we reevaluated our approach to data security and enhanced our security in numerous respects.

Question 2. What have you learned from the incident and what internal steps are you taking to address it from happening again?

Answer. We have learned that the problem of cyber crime is insidious and pervasive, that the hacking community has become increasingly sophisticated and possesses extraordinary ability to assimilate and share information, and that, therefore, a more-coordinated effort among all industry stakeholders is necessary to best address the issue. Along with advocating that type of cooperative approach, as we do here, to guard against future attacks, we have taken various internal steps to enhance the security controls we already had in place, including:

- added additional automated software monitoring and configuration management to help defend against new attacks;
- enhanced levels of data protection and encryption;
- enhanced our capabilities to detect software intrusions within the network, unauthorized access and unusual activity patterns;
- implemented additional layers of firewalls;
- began sharing the knowledge, expertise, and available tools acquired by SNEA during the attack with other Sony companies;
- expedited a planned move of the system to a new data center in a different location with enhanced security; and
- created a new Chief Information Security Officer position at SNEA.

Question 3. What processes have been working for you and what do you need to improve?

Answer. Our communications with our consumers and our Welcome Back program have been working well for us. Our consumers have responded, and we are at or surpass pre-breach metrics for engagement with our customers. We believe that support between industry and government should be improved. Companies are effectively defending against highly sophisticated hackers by themselves with no real means or ability to investigate beyond their own servers if a breach occurs. A strong coalition among government, industry, and consumers is needed to insure that the Internet is not lawless and that online commerce can grow unimpeded. We believe it would be extremely helpful for the public and private sector to develop information-sharing processes that help legitimate business without inadvertently supporting hackers. In addition, means must be found so that consumers, government, and industry can work more closely together to enact strong laws, promote strong enforcement of those laws, and educate consumers about the very real threats that exist online.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. ROGER F. WICKER TO THOMAS M. LENARD, PH.D.

Question 1. In previous hearings of this Committee on online privacy, industry representatives have cited the success of self-regulatory approaches and the importance of enabling flexibility in protecting consumer privacy. In light of these self-regulatory, principles-based efforts, do you think it would be premature for us to move forward with prescriptive regulations?

Answer. There is no evidence that current approaches are not working. Indeed, the recent Department of Commerce Green Paper, which did not recommend prescriptive regulations, observed that "existing U.S. commercial data privacy policy has enabled the digital economy to flourish" (DOC Green Paper, p. 1). This raises questions regarding why that policy should be changed.

Proponents of prescriptive regulation have not thus far demonstrated that there is market failure or that consumers are being harmed under the current regime. Therefore, there is no basis for new regulation. If such a basis were established, there would still be the need to demonstrate that the benefits of any proposed regulation exceed its costs.

Question 2. If we proceed down the path of prescriptive one-size-fits-all regulation do you believe there is a chance it could actually have a reverse effect and compromise providers' ability to protect consumers' personal information?

Answer. Regulating the collection, use and/or retention of data by legitimate firms does little or nothing to deter fraud. It may, however, increase the risk of fraud by making it more difficult for sellers to have the information necessary to determine if a potential buyer is fraudulent.

The ability to authenticate an individual's identity for purposes of online activities will become increasingly important as the Internet develops. Authentication often requires the combination of various sources of data, which is made more difficult (and in some cases, impossible) by various regulatory proposals. Some proposals, such as requiring consumers have access to their data, would also make it easier for fraudsters to access data, thereby making authentication more difficult and increasing the risk of fraud.

If consumers overestimate the risk of online activities—for example, as a result of receiving numerous notices of data breaches—they may be induced to shift their activities offline. This would be exactly the wrong thing to do, because the evidence shows that consumers would reduce their risks by shifting more of their activities online.

○